LỜI CẢM ƠN

Trước hết, em xin bày tỏ lòng biết ơn sâu sắc nhất tới thầy giáo TS Hồ Văn Canh đã tận tình hướng dẫn, giúp đỡ và tạo mọi điều thuận lợi để em hoàn thành tốt đồ án tốt nghiệp của mình.

Em cũng xin chân thành cảm ơn sự dạy bảo của các thầy giáo, cô giáo khoa Công Nghệ Thông Tin trường Đại học Công Nghệ - Đại học Quốc Gia Hà Nội, nơi đã tạo điều kiện tốt trong suốt thời gian thực tập.

Em cũng xin chân thành cảm ơn sự dạy bảo của các thầy giáo, cô giáo khoa công nghệ thông tin -Trường Đại Học Dân Lập Hải Phòng đã trang bị cho em những kiến thức cần thiết trong suốt quá trình học tập, để em có thể hoàn thành đồ án tốt nghiệp.

Xin chân thành cảm ơn các bạn trong lớp đã giúp đỡ và đóng góp ý kiến cho đồ án tốt nghiệp của tôi.

Cuối cùng, em xin được bày tỏ lòng biết ơn tới những người thân trong gia đình đã dành cho em sự quan tâm, động viên trong suốt quá trình học tập và làm tốt nghiệp vừa qua.

Hải Phòng, ngày…tháng 07 năm 2009

Sinh viên

Hoàng Thị Trang

LỜI GIỚI THIỆU

Trong sự phát triển của xã hội loài người, kể từ khi có sự trao đổi thông tin, an toàn thông tin trở thành một nhu cầu gắn liền với nó như hình với bóng. Đặc biệt trong thời đại mà thương mại điện tử đang lên ngôi thì việc có được các công cụ đầy đủ để đảm bảo cho sự an toàn trao đổi thông tin liên lạc là vô cùng cần thiết, đặc biệt là chữ ký số và xác thực. Chính vì vậy chữ ký số đã ra đời với nhiều tính năng ưu việt. Bằng việc sử dụng chữ ký số mà những giao dịch liên quan đến lĩnh vực kinh tế (như giao dịch tài chính, ngân hàng, thuế, hải quan, bảo hiểm…) và những giao dịch yêu cầu tính pháp lý cao (các dịch vụ hành chính công, đào tạo từ xa,...) có thể thực hiện qua mạng máy tính.

Chữ ký số đóng một vai trò quan trọng trong kế hoạch phát triển thương mại điện tử và Chính Phủ điện tử nói chung, trong đó có chữ ký số Liên Bang Nga nói riêng. chữ ký số Liên Bang Nga cung cấp một thuật toán mã hóa có độ mật mềm dẻo, sự cân bằng giữa tính hiệu quả của thuật toán và độ mật của nó. Chuẩn mã dữ liệu của nước Nga đáp ứng được các yêu cầu của các mã pháp hiện đại và có thể chuẩn trong thời gian dài.

Chính vì vậy em đã chọn lĩnh vực “chữ ký số Liên Bang Nga” làm đề tài nghiên cứu cho đồ án tốt nghiệp của mình. Thực sự, đây là một lĩnh vực rất mới đối với Nước ta và là một vấn đề rất khó vì nó liên quan đến các lý thuyết toán học như lý thuyết số, đại số trừu tượng, lý thuyết độ phức tạp tính toán v.v. Với một thời lượng hạn chế mà trình độ em có hạn nên chắc chắn trong luận văn của em còn nhiều thiếu sót, em rất mong được sự chỉ bảo của các thầy, cô để em có thể hoàn thiện tốt hơn nữa luận văn của mình, em xin chân thành cảm ơn.

Mục Lục

Chương 1: Hệ Mật Mã Khóa Công Khai

1.1 Mở đầu

Các vấn đề tồn động của các thuật toán mã hóa đối xứng là lập mã và giải mã đều dùng một khóa do vậy khóa phải được chuyển từ người gửi sang người nhận. Việc chuyển khóa như vậy trên thực tế là không an toàn, vì khóa đó có thể dễ dàng bị ai đó lấy cắp. Để giải quyết vấn đề này vào đầu thập niên 70 một số công trình nghiên cứu đã đưa ra một khái niệm mới về mật mã đó là " Hệ mật mã khóa công khai". Các hệ mật mã này được xây dựng dựa trên cơ sở toán học chặt chẽ, được chứng minh về tính đúng đắn của các thuật toán trong sơ đồ của hệ mã. Và đã giải quyết được vấn đề dùng chung khóa trong các hệ mật mã đối xứng.

Trong các hệ mã hóa công khai, A và B muốn trao đổi thông tin cho nhau thì sẽ được thực hiện theo sơ đồ sau. Trong đó B sẽ chọn khóa k=(k', k"). B sẽ gửi khóa lập mã k' cho A (được gọi là khóa công khai – public key) qua một kênh bất kỳ và giữ lại khóa giải mã k" (được gọi là khóa bí mật – private key). A có thể gửi văn bản M cho B bằng cách lập mã theo một hàm $e_{k'}$ nào đó với khóa công khai k' của B trao cho và được bản mã M' = $e_{k'}$(M). Sau đó gửi M' cho B. Đến lượt B nhận được bản mã M' sẽ dử dụng một hàm giải mã $d_{k'}$ nào đó với khóa bí mật k" để lấy lại bản gốc M=$d_{k"}$(M').

Mật mã khóa công khai xuất hiện năm 1976, do Diffie và Hellman thực hiện năm 1977 ba nhà toán học Revest, Shamir, Adleman đưa ra hệ mã RSA dựa trên độ khó của bài toán phân tích một số tự nhiên lớn thành tích của các số nguyên tố.

1.2 Hệ mật và ví dụ

Mật mã học là sự nghiên cứu các phương pháp toán học liên quan đến khía cạnh bảo mật và an toàn thông tin.

Hệ mật mã: là bộ gồm 5 thành phần (P, C, K, E, D) trong đó:

P (Plaintext): tập hữu hạn các bản rõ có thể.

C (Ciphertext): tập hữu hạn các bản mã có thể.

K (Key): tập hữu hạn các khóa có thể

E (Encrytion): tập các hàm lập mã có thể.

D (Decrytion): tập các hàm giải mã có thể.

Với mỗi $k \in K$, có hàm lập mã $e_k \in E$, $e_k : P \rightarrow C$ và hàm

giải mã $d_k \in D$, $d_k: C \rightarrow P$ sao cho $d_k(e_k(x)) = x$, $\forall x \in P$

Một số hệ mã hóa thường dùng

- Hệ mã khóa đối xứng là hệ mã mà khi ta biết khóa lập mã, "dễ" tính được khóa giải mã. Trong nhiều trường hợp, khóa lập mã và giải mã là giống nhau.

Một số hệ mã hóa đối xứng như : DES, RC2, IDEA v.v

- Hệ mã hóa phi đối xứng: là hệ mã mà khi biết khóa lập mã, "khó" tính được khoá giải mã.

Hệ trên còn được gọi là hệ mã hóa khóa công khai trong đó mỗi người sử dụng một khóa và công bố công khai trên một danh bạ, và giữ bí mât khóa riêng của mình.

Một số hệ mã phi đối xứng: RSA, Elgamal …

Ví dụ:

Hệ mã RSA (Rivest, Shamir, Adleman) mà về sau chúng sẽ được giới thiệu.

1.3 Mật mã DES(Data Encryption Standard)

Mã khối (block cipher) dựa trên nguyên tắc chia bản tin thành các khối, có độ dài bằng nhau, mã từng khối độc lập, trong môi trường máy tính độ dài tính bằng bit.

Mô hình mã khoá bí mật (mã hoá đối xứng) phổ biến nhất đang được sử dụng là DES - Data Encryption Standard được IBM đề xuất và được uỷ ban Chuẩn Quốc gia Mỹ, hiện gọi là Viện Quốc gia về chuẩn và công nghệ (NIST), chấp nhận như một chuẩn chính thức.

DES sử dụng một phép toán hoán vị, thay thế, và một số toán tử phi tuyến. Các phép toán tử phi tuyến này được áp dụng (16 lần) vào từng khối của thông điệp độ dài 64 bit. Bản rõ trước hết, được chia thành các khối thông điệp 64 bit. Khoá sử dụng 56 bit nhận được từ khoá bí mật 64 bit, trừ ra 8 bit ở các vị trí 8,

16, 24, 32, 40, 48, 56, và 64 được dùng để kiểm tra tính chẵn lẻ. Thuật toán giải mã được thực hiện theo chiều ngược lại, với cùng một khoá bí mật đã dùng khi mã hóa.

1.4 Một số hệ mật khóa công khai

1.4.1 Hệ mật RSA

Hệ mật này sử dụng tính toán trong Z_n, trong đó n là tích của 2 số nguyên tố phân biệt p và q. Ta đặt $\phi(n) = (p - 1).(q - 1)$. Ta có định nghĩa sau:

Định nghĩa

Cho n = p*q trong đó p và q là các số nguyên tố phân biệt.

Đặt P = C = Zn

K = {(n, p, q, a, b:a.b$\equiv$ 1 mod n) }, trong đó cặp (n,b) được công khai, còn cặp (n,a) được giữ bí mật mà chỉ có người giải mã mới sở hữu nó.

Mã hóa

Giả sử Alice có một thông báo mật x muốn gửi cho Bob. Alice làm như sau: Cô ta dùng khóa công khai của Bob giả sử là cặp (n,b) và tính:

$y=e_k(x) = x^b \bmod n$ rồi gửi bản mã y cho Bob.

Giải mã

Sau khi nhận được bản mã y từ Alice anh ta tính: $d_k(y) = y^a \bmod n = x$. Đây chính là bản thông báo mật mà Alice gửi cho mình.

Độ mật của hệ mật RSA được dựa trên giả thiết là hàm mã $e_k = x^b \bmod n$ là hàm một chiều. Bởi vậy nhà thám mã sẽ khó có khả năng về mặt tính toán để giải mã một bản mã. Cửa sập cho phép N chính là thông tin về phép phân tích thừa số n (n = p.q). Vì N biết phép phân tích này nên anh ta có thể tính $\phi(n) = (p - 1).(q - 1)$ và rồi tính số mũ giải mã a bằng cách sử dụng thuật toán Euclide mở rộng.

1.4.2 Hệ mật Elgamal

Bài toán logarithm rời rạc trong Z_p

Đặc trưng của bài toán: cho trước cặp bộ ba (p, α, β) trong đó p là số nguyên tố, $\alpha \in Z_p$ là phần tử sinh và $\beta \in Z_p^*$.

Mục tiêu: Hãy tìm một số nguyên duy nhất a, $0 \le a \le p - 2$ sao cho:

$\alpha^a \equiv \beta \pmod p$

Ta sẽ xác định số nguyên a bằng $\log_\alpha \beta$. Nhưng đây được coi là bài toán khó nếu số nguyên tố p đủ lớn.

Định nghĩa mã khóa công khai Elgamal trong Z_p^*:

Cho p là số nguyên tố sao cho bài toán logarithm rời rạc trong Z_p là khó giải. Cho $\alpha \in Z_p^*$ là phần tử nguyên thuỷ. Giả sử $P = Z_p$, $C = Z_p^* \times Z_p^*$. Ta định nghĩa: $K = \{(p, \alpha, a, \beta): \beta \equiv \alpha^a \pmod p\}$

Các giá trị p, α, β được công khai, còn a giữ bí mật mà chỉ có người sở hữu nó mới biết.

Mã hóa

Giả sử Alice có một bản thông báo bí mật $x \in P$ muốn được chia sẽ với Bob. Alice dùng khóa công khai của Bob là (p,α,β) và lấy một số ngẫu nhiên (bí mật) $k \in Z_{p-1}$ rồi tính $e_K(x, k) = (y_1, y_2)$. Trong đó:

$y_1 = \alpha^k \bmod p$

$y_2 = x\beta^k \bmod p$ và gửi y_1, y_2 cho Bob.

Giải mã.

Sau khi nhận được bản mã y_1, y_2 cùng với khóa riêng của mình Bob tính:

$d_k(y_1,y_2) = y_2(y_1^a)^{-1} \bmod p = x$ là bản thông báo mà Alice muốn chia sẽ với mình.

1.4.3 Hệ mật đường cong Elliptic

a. Đường cong Elliptic

Định nghĩa 1a. Cho p>3 là số nguyên tố. Đường cong elliptic

$y^2 = x^3 + ax + b$ trên Z_p là tập các nghiệm $(x,y) \in Z_p \times Z_p$ của đồng dư thức

$y^2 = x^3 + ax + b \pmod p$ (1)

Trong đó $a, b \in Z_p$ là các hằng số thỏa mãn $4a^3 + 27b^2 \neq 0 \pmod p$ (để đa thức $x^3 + ax + b$ không có nghiệm bội) cùng với điểm đặc biệt 0 được gọi là điểm vô hạn.

Định nghĩa 1b. Đường cong Elliptic trên $GF(2^n)$ là tập các điểm

$(x,y) \in GF(2^n) \times GF(2^n)$ thỏa mãn phương trình

$y^2 + y = x^3 + ax + b$ (2)

cùng với điểm vô hạn 0

Định nghĩa 1c. Đường cong Elliptic trên $GF(3^n)$ là tập các điểm

$(x,y) \in GF(3^n) \times GF(3^n)$ thỏa mãn phương trình

$y^2 = x^3 + ax^2 + bx + c$ (3)

cùng với điểm vô hạn 0.

Định lý hasse

Việc xây dựng các hệ mật mã trên đường cong Elliptic bao gồm việc lựa chọn đường cong E thích hợp và một điểm G trên E gọi là điểm cơ sở. Xét trường K là F_q.

N là số điểm của E trên trường F_q (trường hữu hạn q phần tử). Khi đó: $|N - (q+1)| \leq 2\sqrt{q}$. Từ định lý Hasse suy ra $\#E(F_q) = q + 1 - t$ trong đó $|t| \leq 2\sqrt{q}$.

b. Hệ mật trên đường cong Elliptic

Hệ Elgamal làm việc với nhóm Cyclic hữu hạn. Năm 1978, Kobliz đã đưa một hệ trên ECC dựa trên hệ Elgamal.

Để xây dựng hệ mã hoá dựa trên đường cong Elliptic ta chọn đường cong E (a, b) và một điểm G trên đường cong làm điểm cơ sở. Mỗi người dùng A một khoá bí mật n_A là một số nguyên, và sinh khoá công khai $P_A = n_A * G$.

Khi đó hệ mã hoá đường cong Elliptic được xây dựng tương tự hệ mã hoá ElGamal, trong đó thuật toán mã hoá và giải mã được xác định như sau:

Thuật toán mã hoá

Giả sử người dùng A muốn gửi thông điệp cần mã hoá P_m tới người dùng B, chọn một số ngẫu nhiên k và gửi thông điệp mã hoá C_m được tính như sau:

$C_m = \{k * G, P_m + k * P_B\}$

(P_B là khoá công khai của B)

Thuật toán giải mã

Để giải mã thông điệp $C_m = \{ k * G, P_m + k * P_B \}$, người dùng B thực hiện tính như sau:

$P_m + k * P_B - n_B * k * G = P_m + k * P_B – k * n_B * G = P_m + k * P_B - k * P_B = P_m$

Chỉ có B mới có thể giải mã vì B có n_B (là khoá bí mật).

Chú ý rằng ở đây P_m là một điểm thuộc đường cong Elliptic, quá trình mã hoá giải mã được thực hiện trên các điểm thuộc đường cong E. Trong thực tế, để sử dụng được việc mã hóa người ta phải tương ứng một số (tức là bản thông báo) với một điểm thuộc đường cong Elliptic. Khi đó mỗi thông điệp cần mã hoá sẽ tương ứng với một dãy số. Mỗi số sẽ tương ứng với một điểm trên đường cong Elliptic.

Tính bảo mật

Nếu kẻ tấn công giữa đường, Oscar có thể giải bài toán EDLP thì anh ta có thể biết được khoá bí mật từ n_B của B từ các thông tin công khai G và n_BG, và có thể giải mã thông điệp mà A gửi. Như vậy độ an toàn (bảo mật) của thuật toán trên dựa vào độ khó của bài toán EDLP.

Lược đồ trao đổi khóa Diffie-Hellman dùng đường cong Elliptic.

Alice và Bob chọn điểm $B \in E$ để công khai và phục vụ như một điểm cơ sở, B đóng vai trò phần tử sinh của lược đồ Diffie-Hellman trên trường hữu hạn. Để sinh khóa, Alice chọn ngẫu nhiên số a có bậc q rất lớn (nó xấp xỉ N #E) và giữ bí mật, tính $aB \in E$ và công bố nó trên một danh bạ.

Bob làm tương tự chọn ngẫu nhiên b, và công khai $bB \in E$. Không giải bài toán logarit rời rạc, không có cách nào tính được abB khi chỉ biết aB và bB.

c. Logarit rời rạc trên đường cong Elliptic

Định nghĩa:

Nếu E là đường cong Elliptic trên trường F_q và B là một điểm trên E. Khi đó bài toán logarit rời rạc trên E (theo cơ số B) là một bài toán, cho trước một điểm $P \in E$, tìm số nguyên $x \in Z$ sao cho $xB = P$ nếu số x như vậy tồn tại.

Dường như bài toán logarit rời rạc trên đường cong Elliptic khó hơn bài toàn tìm logarit rời rạc trên trường hữu hạn.

d. Chọn đường cong và điểm

Chọn đường cong tức là chọn điểm cơ sở và hệ số a, b sao cho phù hợp vì nó ảnh hưởng tới tốc độ, độ dài khóa và độ an toàn của hệ mật trên đường cong này.

Chọn ngẫu nhiên (E,B). Giả sử p>3 xét Z_p

Trước hết cho x, y, a là 3 phần tử được chọn ngẫu nhiên trên Zp.

Đặt $b=y^2 - (x^3+ax)$, kiểm tra $(4a^3+27b^2 \neq 0)$. Nếu thỏa mãn khi đó B (x,y) là điểm trên đường cong Elliptic $y^2 =x^3 +ax+b$ và ngược lại thì ta hủy bỏ các số đó đi và chọn các số khác...Cứ như vậy cho đến khi ta tìm được các số theo mong muốn.

Chương 2: Chữ Ký Số

2.1 Khái niệm chung

Chữ kí điện tử là thông tin đi kèm theo một tài liệu khác như văn bản, hình ảnh, ... nhằm mục đích xác định người chủ của dữ liệu và đảm bảo tính toàn vẹn của dữ liệu đó. Đồng thời nó còn cung cấp chức năng chống chối bỏ của người gửi thông tin.

So sánh chữ ký thông thường và chữ ký diện tử

Chữ ký thông thường	**Chữ ký điện tử**
Vấn đề ký một tài liệu Chữ ký là một phần vật lý của tài liệu	Vấn đề ký một tài liệu Chữ ký điện tử không gắn kiểu vật lý vào bức thông điệp nên thuật toán được dùng phải "không nhìn thấy" theo một cách nào đó trên bức thông điệp
Vấn đề về kiểm tra Chữ ký kiểm tra bằng cách so sánh nó với chữ ký xác thực khác. Tuy nhiên, đây không phải là một phương pháp an toàn vì nó dễ bị giả mạo.	Vấn đề về kiểm tra Chữ ký điện tử có thể kiểm tra nhờ dùng một thuật toán "kiểm tra công khai". Như vậy, bất kì ai cũng có thể kiểm tra được chữ ký điện tử. Việc dùng chữ ký điện tử an toàn có thể chặn được giả mạo.
Bản copy thông điệp được ký bằng chữ ký thông thường lại có thể khác với bản gốc.	Bản copy thông điệp được ký bằng chữ ký điện tử thì đồng nhất với bản gốc, điều này có nghĩa là cần phải ngăn chặn một bức thông điệp ký số không bị dùng lại.

Sơ đồ kí điện tử gồm 5 thành phần (P, A, K, S, V) trong đó:

P là tập hữu hạn các văn bản có thể.

A là tập hữu hạn các chữ ký có thể.

K là tập hữu hạn các khóa có thể.

Với $k \in K$, $k = (k', k'')$, k' là khoá bí mật để kí và

k'' là khoá công khai để kiểm thử chữ kí.

S là tập các thuật toán kí có thể.

V là tập các thuật toán kiểm thử.

Với mỗi $k \in K$, có thuật toán ký $sig_{k'} \in S$, $sig_k: P \rightarrow A$ và thuật toán kiểm thử $ver_{k''} \in V$, $ver_{k''}: P \times A \rightarrow$ {đúng, sai}, thoả mãn điều kiện sau đây với mọi $x \in P$, $y \in A$:

$ver_{k''}(x,y) =$ đúng, nếu $y = sig_{k'}(x)$

sai, nếu $y \neq sig_{k'}(x)$

Một số chữ kí điện tử: RSA, Elgamal, DSS, ...

2.2 Một vài lược đồ chữ ký số tiêu biểu

2.2.1 Lược đồ chữ ký RSA

Lược đồ chữ ký RSA được định nghĩa như sau:

- Tạo khóa:

Sơ đồ chữ ký cho bởi bộ năm (P, A, K, S, V)

Cho n=pq, với mỗi p, q là các số nguyên tố lớn khác nhau

$\phi(n) = (p - 1)(q - 1)$.

Cho $P = A = Z_n$ và xác định:

$K = \{(n, p, q, a, b): ab \equiv 1 (\mod \phi(n)) \}$

Các giá trị n, b là công khai các giá trị p, q, a là các giá trị bí mật.

- Tạo chữ ký:

Với mỗi K=(np, q, a, b) xác định:

$Sig_{K'}(x) = x^a \mod n$

- Kiểm tra chữ ký:

$Ver_{K''}(x,y) = true \Leftrightarrow x \equiv y^b \mod n$; $x, y \in Z_n$.

Giả sử A muốn gửi thông báo x, A sẽ tính chữ ký y bằng cách :

$y = sig_{K'}(x) = x^a \mod n$ (a là tham số bí mật của A)

A gửi cặp (x,y) cho B. Nhận được thông báo x, chữ ký số y. B bắt đầu tiến hành kiểm tra đẳng thức $x= y^b \bmod(n)$ (b là khóa công khai A).

Nếu đúng, B công nhận y là chữ ký trên x của A. Ngược lại, B sẽ coi x hoặc là đã bị sửa chữa, hoặc là chữ ký bị giả mạo. Người ta có thể giả mạo chữ ký của A như sau: chọn y sau đó tính

$x= ver_{K''}(y)$, khi đó $y= sig_{K'}(x)$. Một cách khắc phục khó khăn này là việc yêu cầu x phải có nghĩa. Do đó chữ ký giả mạo thành công với xác suất rất nhỏ.

Hơn nữa, việc sử dụng hàm hash liên kết với lược đồ chữ ký loại bỏ phương pháp giả mạo.

2.2.2 Lược đồ chữ ký Elgamal

Lược đồ chữ ký ElGamal được đề xuất năm 1985, gần như đồng thời với sơ đồ hệ mật mã ElGamal, cũng dựa trên độ khó của bài toán lôgarit rời rạc. Lược đồ được thiết kế đặc biệt cho mục đích ký trên các văn bản điện tử, được mô tả như một hệ: $S=(P, A, K, S, V)$

Trong đó $P = Z^*_p$, $A = Z^*_p \times Z_{p-1}$, với p là một số nguyên tố sao cho bài toán tính lôgarit rời rạc trong Z^*_p là rất khó. Tập hợp K gồm các cặp khoá K=(K', K''), với K'=a là một số bí mật thuộc Z^*_p, K'' =(p, α, β), α là một phần tử nguyên thuỷ của Z^*_p, và $\beta=\alpha^a \bmod p$. K' là khoá bí mật dùng để ký, và K'' là khoá công khai dùng để kiểm thử chữ ký.

Lược đồ chữ ký ElGamal được định nghĩa như sau:

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trong Z_p là khó và giả sử $\alpha \in \mathbf{Z}^*_p$ là phần tử nguyên thủy

Cho $P = Z^*_p$, $A = Z^*_p \times Z_{p-1}$ và định nghĩa

$K = \{(p, a, \alpha, \beta): \beta = \alpha^a \bmod p \}$.

Các giá trị p, α, β là công khai, a là bí mật.

*Tạo chữ ký.

Giả sử x là một thông báo cần ký. Khi đó, với K = (p, a, α, β) và với số ngẫu nhiên $k \in Z^*_{p-1}$, ta định nghĩa chữ ký số ElGamal là cặp (γ, δ), trong đó:

$\gamma = \alpha^k \bmod p$ và $\delta = (x - a\gamma)\, k^{-1} \bmod (p - 1)$.

*Kiểm tra chữ ký số.

Với x, $\gamma \in Z^*_p$, và $\delta \in Z_{p-1}$ ta định nghĩa :

Ver (x, γ, δ) = True $\Leftrightarrow \beta^{\gamma}.\gamma^{\delta} \equiv \alpha^x \bmod p$.

2.2.3 Lược đồ chuẩn chữ ký số DSS (Digital Signature Standard Algorithm)

Sơ đồ chữ ký DSS được cho bởi bộ năm

$S = (P, A, K, S, V)$

Trong đó $P = Z^*_p$, $A = Z^*_q \times Z^*_q$

p là một số nguyên tố lớn có độ dài biểu diễn $512 \le l_p \le 1024$ bit (với l là bội của 64) sao cho bài toán tính logarit rời rạc trong Z_p* là khó.

q là một ước số nguyên tố của p -1 có l_q biểu diễn cỡ 160 bit.

Gọi $\alpha \in Z^*_p$, $\alpha = \alpha_o^{(p-1)/q} \bmod p \neq 1$ với 1<h<p-1(với α_o một phần tử nguyên thủy trong Z_p*)

a là số ngẫu nhiên (0 < a < q)

$\beta \equiv \alpha^a \bmod p$.

k là số ngẫu nhiên (0 < k < q)

K=(K', K"), trong đó khoá bí mật K' = a, và khoá công khai K" = (p, q, α, β)

- Hàm ký $sig_{k'}$: $sig_{k'}(x,k) = (\gamma, \delta)$ là chữ ký trên thông điệp x.

Trong đó $\gamma = (\alpha^k \bmod p) \bmod q$

$\delta = (x + a\gamma)k^{-1} \bmod q$.

- Hàm kiểm thử $ver_{k''}$: $ver_{k''}(x,(\gamma, \delta))$

- Tính : $e_1 = x\, \delta^{-1} \bmod q$

$e_2 = \gamma\, \delta^{-1} \bmod q$

- Kiểm tra đẳng thức: $(\alpha^{e1}\, \beta^{2} \bmod p) \bmod q = \gamma$?

+Nếu có đẳng thức : chữ ký tin cậy

+ Nếu không : chữ ký số không tin cậy hoặc thông điệp x đã bị sữa đổi

2.2.4 Hàm hash và ứng dụng trong chữ ký số

Định nghĩa : Giả sử D là tập các văn bản có thể. X là tập các văn bản tóm lược (đại diện) có thể với độ dài cố định trước tùy ý. Việc tìm cho mỗi văn bản một tóm lược tương ứng xác định một hàm h: D→ X. Hàm h như vậy được gọi là hàm băm.

Hàm băm thường phải thỏa mãn các điều kiện sau:

+ Hàm băm phải là hàm không va chạm mạnh:

Không có thuật toán tính trong thời gian đa thức để có thể tìm được $x_1, x_2 \in D$ sao cho $x_1 \neq x_2$ và $h(x_1) = h(x_2)$.

Tức là tìm 2 văn bản khác nhau có cùng đại diện là rất "khó".

+ Hàm băm là hàm một phía:

Tức là cho x tính z = h(x) thì "dễ", nhưng biết z tính x là "khó".

+ Hàm băm phải là hàm không va chạm yếu:

Tức là cho $x \in D$, khó tìm được $x' \in D$, $x' \neq x$ và $h(x) = h(x')$.

Một số hàm hash sử dụng trong chữ ký số.

Các hàm Hash đơn giản:

Tất cả các hàm Hash đều được thực hiện theo quy tắc chung là: Đầu vào được biểu diễn dưới dạng một dãy tùy ý các khối n bit, các khối n bit này được xử lý theo cùng một kiểu và lặp đi lặp lại để cuối cùng cho đầu ra có số bit cố định.

Hàm Hash đơn giản nhất là thực hiện phép toán XOR từng bit một của mỗi khối. Nó được biểu diễn như sau:

$C_i = b_{1i} \oplus b_{2i} \oplus \ldots \oplus b_{mi}$ Trong đó

C_i : là bit thứ i của mã Hash, $i = \overline{1,n}$

m : là số các khối đầu vào

b_{ji} : là bit thứ i trong khối thứ j

$\oplus$: là phép cộng modulo 2

Sơ đồ hàm Hash sử dụng phép XOR.

Khối 1:	b_{11}	b_{12}	…	b_{1n}
Khối 2:	b_{21}	b_{22}	…	b_{2n}
…	…	…	…	…
Khối m:	b_{m1}	b_{m2}	…	b_{mn}
Mã Hash:	C_1	C_2	…	C_n

C_i là bit kiểm tra tính chẵn lẻ cho vị trí thứ i khi ta chia tệp dữ liệu thành từng khối, mỗi khối con vị trí. Nó có tác dụng như sự kiểm tra tổng thể tính toàn vẹn của dữ liệu.

Khi mã hóa một thông báo dài thì ta sử dụng mode CBC (The Cipher Block Chaining), thực hiện như sau:

Giả sử thông báo X được chia thành các khối 64 bit liên tiếp

$X= X_1X_2 \dots X_n$

Khi đó mã Hash C sẽ là: $C = X_{NH} = X_1 \oplus X_2 \oplus \dots \oplus X_n$

Sau đó mã hóa toàn bộ thông báo nối với mã Hash theo mode CBC sản sinh ra bản mã $Y_1Y_2 \dots Y_{N+1}$

Kỹ thuật khối xích :

Người đầu tiên đề xuất kỹ thuật mật mã xích chuỗi nhưng không có khóa bí mật là Rabin.

Kỹ thuật này được thực hiện như sau :

Chia thông báo M thành các khối có cỡ cố định là $M_1, M_2, \dots, M_N$, sử dụng hệ mã thuận tiện như DES để tính mã Hash như sau :

H_0 = giá trị ban đầu

$H_i = E_{Mi}(H_{i-1})$, i = 1,2....N, G= H_N

Ở trên ta đề cập đến hàm Hash có nhiều đầu vào hữu hạn. Tiếp theo ta sẽ đề cập tới loại hàm Hash mạnh với đầu vào vô hạn thu được do mở rộng một hàm Hash mạnh có đầu vào độ dài hữu hạn. Hàm này sẽ cho phép ký các thông báo có độ dài tùy ý.

Giả sử h: $(Z_2)^m \rightarrow (Z_2)^t$ là một hàm Hash mạnh, trong đó $m \geq t + 1$ ta sẽ xây dựng một hàm Hash mạnh :

$h^*: X \rightarrow (Z_2)^t$, trong đó $X = \cup(Z_2)^i$

❖ Xét trường hợp $m \geq t + 2$

Giả sử $x \in X$, vậy thì tồn tại n để $x \in (Z_2)^n$, $n \geq m$.

Ký hiệu : |x| là độ dài của x tính theo bit. Khi đó |x| = n.

Ký hiệu : x||y là dãy bit thu được do nối x với y.

Giả sử $|x| = n \geq m$. Ta có thể biểu diễn x như sau: $x = x_1||x_2|| \ldots||x_k$

trong đó $|x_1| = |x_2| = \ldots = |x_k| = m-t-1$ và $|x_k| = m-t-d$, $0 \leq d \leq m-t-2$

(do đó $|x_k| \geq 1$ và $m-t-1 \geq 1$, $k \geq 2$)

Thế thì $k = [n/(m-t-1)]+1$; ([] : chỉ phần nguyên)

Thuật toán xây dựng h thành h* được mô tả như sau :

1. Cho i = 1 tới k-1 gán $y_i = x_i$;
2. $y_k = x_k \,||\, 0^d$ (0^d là dãy có d số 0, khi đó y_k dài m-t-1)
3. y_{k+1} là biểu diễn nhị phân của d ($|y_{k+1}| = m-t-1$)
4. $g_1 = h(0^{t+1} || y_1)$ ($g_1 = t$, $0^{t+1} || y_1$ dài m)
5. Cho i=1 tới k thực hiện $g_{i+1} = h(g_i || 1 || y_{i+1})$
6. $h^*(x) = g_{k+1}$, Ký hiệu $y(x) = y_1 \,||\, y_2 \,||\ldots||\, y_{k+1}$

Ta thấy rằng $y(x) \neq y(x')$ nếu $x \neq x'$

Thuật toán MD5

Thuật toán MD5 được Ron Rivest đưa ra vào năm 1991. Đầu vào của thuật toán là các khối có độ dài 512 bit và đầu ra là một bản băm đại diện cho văn bản gốc có độ dài 128 bit.

Các bước tiến hành :

Bước 1 : Độn thêm bit

Bước 2 : Thêm độ dài

Bước 3 : Khởi tạo bộ đệm của MD

Bước 4 : Tiến trình thực hiện

Bước 5 : Đầu ra

Chương 3: Chuẩn Chữ Ký Số Của Liên Bang Nga

3.1 Lời giới thiệu

Ngày 10 tháng 4 năm 2002, tổng thống Nga V.Putin đã ký sắc lệnh Liên Bang về chữ ký điện tử số.

Luật về chữ ký điện tử số được nước Nga chuẩn bị kỹ từ trước khi ra các bài báo "Những công nghệ hứa hẹn trong lĩnh vực chữ ký điện tử số", và "Chữ ký điện tử hay con đường gian khổ thoát khỏi giấy tờ".

Nước Nga đã sử dụng chuẩn chữ ký số GOST P34.10-94, chuẩn chữ ký số GOST P34.10-2001 và chuẩn hàm băm GOST P34.10-94.

Việc tìm hiểu chuẩn mật mã nước Nga và Mỹ là quan trọng nhất.

3.2 Chuẩn chữ ký số GOST 34.10 – 94

Chuẩn chữ ký số của Nga được lập sau phương án chuẩn của nước Mỹ, cho nên các tham số của thuật toán này được chọn với trù tính về khả năng tiềm tàng của người mã thám trong việc thám mã. Nói riêng, việc tăng độ dài giá trị hàm băm làm giảm xác xuất đụng chạm, tương ứng với nó là bậc của phần tử sinh, điều này làm cho việc giải bài toán logarithm rời rạc sẽ khó hơn khi cần tìm khóa bí mật.

a.Chọn tham số

Để mô tả thuật toán sử dụng các ký hiệu sau :

B* - tập tất cả các từ hữu hạn trên bảng chữ cái B={0,1};

|A| - Độ dài từ A;

V_k (2) - tập tất cả các từ nhị phân độ dài k;

A||B - nối hai từ A và B (hay còn ký hiệu là AB);

A^k - nối k từ A liên tiếp;

<N>k - từ có độ dài k là kết quả của phép tính N (mod 2k) với N là số nguyên không âm.

$\oplus$ - phép cộng từng bít theo mudulo 2;

[+] - phép cộng theo quy tắc A [+] B=$<A+B>_k$ (k=|A|=|B|);

m - thông báo cần ký;

m_1 - thông báo nhận được;

h - hàm băm ánh xạ dãy m vào từ h(m) ϵ $V_{256}(2)$;

p - số nguyên tố, $2^{509} < p < 2^{512}$, hoặc $2^{1020} < p < 2^{1024}$

q - số nguyên tố, $2^{254} < p < 2^{556}$, và q là ước của (p-1);

a - số nguyên, 1<a<p-1, với $a^q(\text{mod } p)=1$;

k - số nguyên, 0<k<q;

x - khóa bí mật của người sử dụng để ký, 0<x<q;

y - khóa công khai để kiểm tra chữ ký $y = a^x \text{ (mod } p)$;

Các số p, q và a là các tham số của hệ thống, được công bố công khai. Bộ giá trị cụ thể có thể là chung cho tất cả mọi người trong hệ thống. Số k được sinh trong quá trình ký thông báo cần phải giữ bí mật và được hủy ngay sau khi ký. Số k được lấy từ bộ tạo ngẫu nhiên vật lý hoặc bởi dãy giả ngẫu nhiên với các tham số bí mật.

b.Tạo chữ ký

Việc tạo chữ ký gồm các bước sau:

1) Tính h(m) - giá trị hàm băm của thông báo m . Nếu h(m)(mod q) = 0

thì gán cho h(m) giá trị $0^{255}1$;

2) Chọn số nguyên k, 0<k<q;

3) Tính hai giá trị $r'=a^k(\text{ mod } p)$ và r=r'(mod q). Nếu r=0 chuyển về bước 2 và chọn lại giá trị k khác;

4) Người sử dụng dùng khóa bí mật x để tính giá trị s=(xr+kh(m))(mod q).

Nếu s=0 thì chuyển về bước 2, trong trường hợp ngược lại thì kết thúc thuật toán.

Chú ý rằng thông báo cho giá trị hàm băm bằng 0 không được ký. Trong trường hợp ngược lại phương trình ký sẽ được giản ước thành s=xr (modq) và người ác ý sẽ tính được khóa bí mật.

c. Kiểm tra chữ ký

Phương trình kiểm tra là $r=(a^{s.h(m1)-1}. y^{-r.h(m1)-1} (\text{mod } p))(\text{mod } q)$. Thực vậy $(a^{s.h(m)-1} . y^{-r.h(m)-1} (\text{mod } p))(\text{mod } q)= (a^{s.h(m)-1} . a^{-r.x.h(m)-1} (\text{mod } p))(\text{mod } q)$ $=(a^{h(m)-1\,(s - r.x)}(\text{mod } p)) (\text{mod } q) =a^{h(m)-1\,(x.r + kh(m) - r.x)}(\text{mod } p)(\text{mod } q)$ $=a^{h(m)-1\,.kh(m)}(\text{mod } p)(\text{mod } q) = a^k (\text{mod } p)(\text{mod } q) \equiv r$.

Việc tính toán được thực hiện như sau:

1) Kiểm tra điều kiện: $0<s<q$ và $0<r<q$. Nếu một trong những điều đó không được thực hiện coi như chữ ký không có hiệu lực hoặc thông báo ký đã bị sửa chữa.

2) Tính $h(m_1)$ giá trị hàm băm của bản tin nhận được. Nếu $h(m_1)(\text{mod } q)=0$ thì gán cho $h(m_1)$ giá trị $0^{255}1$.

3) Tính $v=(h(m_1))^{q-2}(\text{mod } q)$. Chính là việc tính $h(m_1)^{-1}(\text{mod } q)$ bằng thuật toán Eucolid mở rộng sẽ nhanh hơn việc nâng lũy thừa.

4) Tính $z_{1=}s.v(\text{mod } q)$ và $z_2=(q-r).v(\text{mod } q)$

5) Tính $u =(a^{z1} . y^{z2} (\text{mod } p))(\text{mod } q)$

6) Kiểm tra điều kiện r = u. Nếu đẳng thức xảy ra thì công nhận chữ ký đúng và bản tin không bị thay đổi trong quá trình truyền.

3.3 Chuẩn chữ ký số GOST P34.10 – 2001

Do sự tăng năng suất của các phương tiện tính toán và việc hoàn thiện thuật toán tính logarit rời rạc trong trường hữu hạn nên xuất hiện nhu cầu tăng độ bền vững của thuật toán chữ ký điện tử số đối với nhiều dạng tấn công. Vì thế nên chuẩn GOST P34.10 - 2001 đã được nghiên cứu trong dự án "Công nghệ thông tin. Bảo vệ thông tin bằng mật mã. Các quá trình tạo và kiểm tra chữ ký điện tử số". Nó sẽ được áp dụng từ ngày 1 tháng 7 năm 2002 thay cho chuẩn GOST P34.10 – 94 trước đó.

a. Chuẩn bị tham số

Trong chuẩn này các phép toán của nhóm các điểm thuộc đường cong Elliptic trên trường hữu hạn được sử dụng. Đường cong Elliptic E trên trường nguyên tố

GF(p) được sử dụng, nó được cho bởi các hệ số a và b hoặc đại lượng J(E) được gọi là bất biến đường cong : $J(E)=1728\frac{4a^3}{4a^3+27b^2} \bmod p$. Các hệ số a và b của đường cong E được xác định thông qua hằng số bởi công thức:

Với $a \equiv 3k \bmod p$; $b \equiv 2k \bmod p$; $k=\frac{-J(E)}{1728-J(E)} \bmod p$, ($J(E) \neq 0,1728$).

Điểm Q được gọi là điểm bội k, $k \in z$ nếu như với một điểm P nào đó có đẳng thức Q=kP. Các tham số của lược đồ chữ ký số bao gồm:

p - số nguyên tố là modulo của đường cong Elliptic (E), $p>2^{255}$

Đường cong E được cho bởi bất biến J(E), hay các hệ số a, b

m -số nguyên bậc của nhóm các điểm trên đường cong E

q -số nguyên tố bậc của nhóm vòng con của nhóm các điểm thuộc đường cong E với điều kiện

$$\begin{cases} m = nq, n \in Z, n \geq 1 \\ 2^{254} < q < 2^{256} \end{cases}$$

$P \neq 0$ điểm cơ sở trên đường cong có bậc q, tức là pQ=0 tọa độ điểm này ký hiệu qua (x_p, y_p).

Hàm băm ánh xạ thông báo có độ dài bất kỳ vào tập các vectơ nhị phân độ dài 256. Hàm băm được định nghĩa bởi chuẩn GOST P34.10 - 94.

Mỗi người sử dụng lược đồ chữ ký điện tử cần có cặp khóa cá nhân sau:

Khóa bí mật của người sử dụng - số nguyên d, 0< d< q;

Khóa công khai của người sử dụng - điểm Q với tọa độ (x_q, y_q), thỏa mãn đẳng thức dP=Q.

Các tham số của chữ ký điện tử cần thỏa mãn

$p^t \neq 1 \pmod q$ với mọi t=1,2,.....,B với $B \geq 31$;

$m \neq p$;

$J(E) \neq 0$ hay 1728.

Chúng ta đặt tương ứng vectơ nhị phân $\bar{h}=(\alpha_{255},.....,\alpha_0)$ với số $\alpha=\sum_{i=0}^{255} \alpha_i 2^1$

b. Sinh chữ ký số

Chữ ký số cho bản tin M được tính như sau:

1.Tính hàm băm: $\bar{h}$=h(M)

2.Tính số nguyên α có dạng biểu diễn nhị phân là vecto $\bar{h}$ và xác định e ≡α(mod q). Nếu e=0 thì gán e=1.

3. Sinh ra số giả ngẫu nhiên k thỏa mãn bất đẳng thức 0<k<q.

4. Tính điểm thuộc đường cong Elliptic C=kP và đặt r≡x_c(mod q) với x_c tọa độ của điểm C theo trục X. Nếu r=0 thì quay về bước 3.

5. Tính giá trị s=(rd+ke)(mod q). Nếu s=0 thì quay về bước 3.

6. Tính vectơ nhị phân ứng với các số s và r. Chữ ký số ζ =($\bar{r}||\bar{s}$) là phép nối 2 vectơ nhị phân.

Kiểm tra chữ ký : Làm như sau

1.Theo chữ ký nhận được ζ cần tính ra hai số nguyên r và s. Nếu các bất đẳng thức sau không đúng thì bác bỏ chữ ký 0<r<q, 0<s<q.

2. Tính hàm băm của bản tin nhận được $\bar{h}$=h(M).

3. Tính số nguyên có dạng biểu diễn nhị phân là vectơ $\bar{h}$ và xác định e≡ α (mod q). Nếu e=0 thì lấy e =1.

4.tính v≡ e^{-1}(mod q).

5.Tính z_1≡s.v (mod q), z_2≡ -rv(mod q)

6.Tính điểm trên đường cong Elliptic C=z_1P+z_2Q, xác định R ≡x_c(mod q) với x_c là tạo độ của điểm C trên trục x.

7.Chữ ký được công nhận khi và chỉ khi R =r.

3.4 chuẩn hàm băm GOST P34.11 - 94

Một số ký hiệu :

M - là dãy nhị phân cần băm ;

h - là hàm băm ánh xạ dãy M từ h(M) ∈V_{256}(2),

E_k(A) kết quả phép băm từ A với khóa bởi thuật toán mã khối Gost 28147-89 ở chế độ thay thế đơn giản ;

H là vectơ khởi điểm để băm.

Mô tả chung

Chúng ta hiểu hàm băm là một ánh xạ h: $B^* \rightarrow V_{256}(2)$

Để định nghĩa hàm băm ta cần có

- Thuật toán tính băm theo từng bước k

K: $V_{256}(2) \times V_{256}(2) \rightarrow V_{256}(2)$

- Mô tả quá trình lặp để tính giá trị hàm băm

a. Thuật toán tính băm theo từng bước gồm 3 phần

Tạo 4 khóa có 256 bit.

Biến đổi mã: sử dụng thuật toán Gost 28147-89 ở chế độ thay thế đơn giản.

Ánh xạ xáo trộn kết quả mã.

Tạo khóa

Xét $X=(b_{256}, b_{255},.....,b_1) \in V_{256}(2)$

Giả sử $X=x_4 ||x_3||x_2||x_1 = \eta_{16}||\eta_{15}||.....||\eta_1= \zeta_{32}||\zeta_{31}||.....||\zeta_1$

Với $x_i \in V_{64}(2)$, i=1….4; $\eta_j \in V_{16}(2)$, j=1……16; $\zeta k \in V_8(2)$, k=1…32.

Ký hiệu $A(X)=(x_1 \oplus x_2)||x_4||x_3||x_2$.

Biến đổi P: $V_{256}(2) \rightarrow V_{256}(2)$ chuyển từ $\zeta_{32}||\zeta_{31}||.....||\zeta_1$ thành từ

$\zeta\varphi(32)||\ \zeta\varphi(31)||.....||\zeta\varphi(1)$ với $\varphi\ (i+1+4(k-1))=8i + k$, i =0..8.

Để tạo khóa cần sử dụng các dữ liệu sau:

- Các từ H, M $\in V_{256}(2)$;
- Các hằng số: Các từ C_i(i=2, 3, 4) có các giá trị $C_2=C_4=0^{256}$ và

$C_3 =1^8 0^8 1^{16} 0^{24} 1^{16} 0^8 (0^8 1^8)^2 1^8 0^8 (0^8 1^8)^4 (1^8 0^8)^4$

Thuật toán tính khóa như sau:

1. Gán các giá trị i=1, U = H, V= M
2. Thực hiện $W=U \oplus V$, $K_1=P(W)$
3. Gán i=i+1
4. Kiểm tra điều kiện i=5. Nếu đúng nhảy bước 7, sai thì tiếp bước 5
5. Tính $U=A(U) \oplus C_i$, $V=A(V(A))$, $W=U \oplus V$, $K_i=P(W)$
6. Chuyển về bước 3

7. Kết thúc

Biến đổi mã

Đây là giai đoạn mã 4 từ con 64 bit của từ H bởi các khóa K_i (i=1,2,3,4). Chúng ta cần các dữ liệu sau: $H=h_4||h_3||h_2||h_1$, $h_i \in V_{64}(2)$ và bộ khóa K_i (i=1,2,3,4)

Sau khi mã ta có $s_i=E_{Ki}(h_i)$, i =1,2, 3,4 và vecto kết quả $S= s_4||s_3||s_2||s_1$

Biến đổi trộn

Trộn dãy thu được qua thanh dịch, dữ liệu ban đầu là các từ H, M, $S \in V_{256}(2)$;

Biến đổi ψ : $V_{256}(2) \rightarrow V_{256}(2)$ chuyển từ $\eta_{16}||\eta_{15}||...||\eta_1 \in V_{64}(2)$, i=1...16 thành từ

$\eta_1 \oplus \eta_2 \oplus \eta_3 \oplus \eta_{13} \oplus \eta_{16}||\eta_{16}||\ \eta_{15}||...||\ \eta_2$. Khi đó giá trị băm từng bước là từ

$K(M,H)= \psi^{16}(H \oplus \psi(M \oplus \psi^{12}(S)))$ Với ψ^i là biến đổi làm i lần.

b. Tính giá trị băm

Giá trị băm ban đầu để tính giá trị hàm băm là dãy $M \in B^*$. Tham số là vectơ khởi điểm H - Một từ cố định tùy ý từ $V_{256}(2)$.

Thủ tục tính hàm h ở mỗi vòng lặp sử dụng các đại lượng sau:

$M \in B^*$ - phần của dãy M, chưa đi qua hàm băm ở những vòng lặp trước

$H \in V_{256}(2)$ - giá trị hiện tại của hàm băm

$\sum \in V_{256}(2)$ - giá trị hiện tại của tổng kiểm tra

$L \in V_{256}(2)$ - giá trị hiện tại của độ dài phần của dãy M xử lý ở các vòng lặp trước

Thuật toán tính hàm h được chia làm 3 giai đoạn:

Giai đoạn 1. Gán các giá trị ban đầu cho các đại lượng hiện tại

M:= M; H:=H; $\sum$:=0256 ; L:=0^{256}

Giai đoạn 2. Kiểm tra điều kiện |M|>256. Nếu đúng chuyển sang bước 3. Ngược lại thì thực hiện các phép tính sau:

L:=<L+|M|>$_{256}$; $\sum$:=$\sum$[+]M' ; M':=$0^{256-|M|}$||M;

H:=$_K$M', H); H:=$_K$L, H); H:=$_K\sum$, H)

Kết thúc thuật toán H là giá trị hàm băm.

Giai đoạn 3. Tính từ con $M_s \in V_{256}(2)$ của từ $M(M=M_p||M_s)$. Tiếp tục thực hiện dãy phép tính sau.

$H:=_K(M', H)$; $L:=<L+256>_{256}$; $\sum = \sum[+]\ M_s$; $M:=M_p$.

Chuyển lên bước 2.

3.5 Chuẩn mã dữ liệu GOST 28147 - 89

Tại Liên Bang Nga có một chuẩn mã duy nhất cho các hệ thống thông tin. Nó là bắt buộc cho các cơ quan nhà nước, tổ chức, xí nghiệp, ngân hàng và các công sở khác có hoạt động gắn liền với việc đảm bảo an toàn thông tin quốc gia. Đối với các tổ chức khác hay các cá nhân thì GOST 28147 -89 mang tính khuyến cáo.

Chuẩn này được thiết lập có tính đến kinh nghiệm trên thế giới, nói riêng đã chú ý đến những điểm yếu và khả năng không thực hiện được của DES, vì vậy việc áp dụng chuẩn có tiện hơn.Thuật toán xây dựng theo cấu trúc Feistel.

Đối với phép nối ta dùng ký hiệu như phép nhân. Ngoài ra ta sử dụng các phép cộng sau:

$A \oplus B$ Phép cộng từng bit theo modulo 2;

$A [+] B$ cộng theo modulo 2^{32};

$A \{+\} B$ cộng theo modulo $2^{32}-1$;

Thuật toán có một số chế độ làm việc. Trong mọi chế độ đều sử dụng khóa W có 256 bit, đó là 8 số có 32 bit: W=X(7)X(6) X(5) X(4) X(3) X(2) X(1) X(0). Khi giải mã chúng ta dùng khóa đó.

Chế độ làm việc cơ sở của thuật toán là chế độ thay thế đơn giản .

Các ký hiệu trên hình vẽ:

N_1, N_2 các thanh ghi lưu 32 bit;

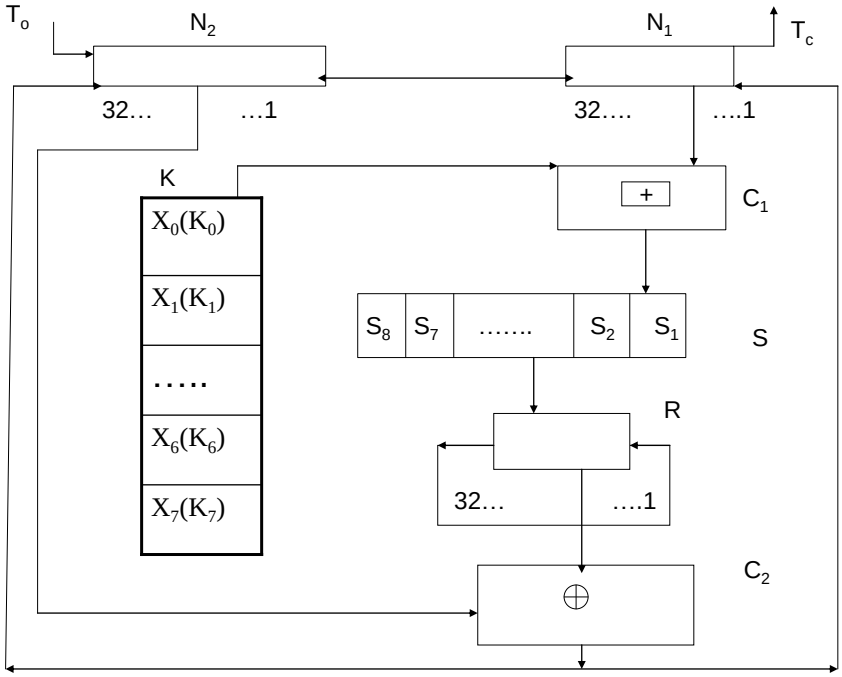
S_1 tổng theo modulo$2^{32;}$

S_2 tổng theo modulo$2^{;}$

N thanh ghi dịch vòng 32 bit;

K thiết bị nhớ khóa gồm 256 bit được chia thành 8 từ 32 bit;

S khối thay thế gồm 8 hộp thế $S_{1,}\ldots,S_{8.}$



Mô tả chế độ làm việc của thuật toán là chế độ thay thế đơn giản

Giả sử bản rõ được chia thành các khối có 64 bit, chúng được ký hiệu là T_o. Thủ tục mã gồm 32 vòng. Đầu tiên, khóa k có 256 bit được đưa vào thiết bị nhớ khóa, tạo thành 8 khóa con k_i: $k=k_7k_6 \ldots..k_1$.

Dãy các bit của T_o được phân thành 2 nửa có 32 bit trái và phải :

$T_o=(a_1(0), a_2(0),\ldots, a_{32}(0), b_1(0), b_2(0),\ldots., b_{32}(0))$.

Các bit trong mỗi nửa được lấy ra theo thứ tự ngược lại để tạo nên hai từ có 32 bit là a(0) và b(0):

$a(0)=(a_{32}(0), a_{31}(0),\ldots, a_1(0))$,

$b(0)=(b_{32}(0), b_{31}(0),\ldots., b_1(0))$.

Hai vectơ 32 bit a(0) và b(0) được đưa vào thanh ghi lưu N_1, N_2 trước vòng mã thứ nhất. a(0) trong N_1 và b(0) trong N_2.

Giả sử $a(j)=(a_{32}(j), a_{31}(j),\ldots, a_1(j))$, $b(j)=(b_{32}(j), b_{31}(j),\ldots., b_1(j))$. Là nội dung của các thanh ghi lưu N_1 và N_2 sau vòng mã thứ j. Chúng ta ký hiệu f là hàm mã, ta có

Với j=1.....24

$a(j)=f(a(j-1)+k_{j-1(\mathrm{mod}\ 8)}) \oplus b(j-1)$

b(j)=a(j-1)

Với j=25....31

$a(j)=f(a(j-1)+k_{32-j \pmod 8}) \oplus b(j-1)$

b(j)=a(j-1)

Với j=32

a(32)=a(31)

$b(32)= f(a(31)+k_0) \oplus b(31)$

Việc tính hàm mật mã f qua 2 giai đoạn:

- Ở giai đoạn thứ nhất, tham số x có 32 bit được chia thành 8 vectơ có 4 bit. Bộ 4 bit thứ i được ánh xạ thành 4 bit nhờ các phép thế $S_i(i=1..8)$. S_i là các phép hoán vị của tập các số nguyên từ 0 đến 15, S(x) là một vectơ có 32 bit.
- Giai đoạn thứ 2: Nhờ thanh ghi R, S(x) được dịch vòng về bên trái 11 vị trí.

Kết quả của phép mã T_o là T_c được lấy ra từ các thanh ghi lưu N_1 và N_2 sau 32 vòng mã theo thứ tự từ trái qua phải.

$T_c=(a_1(32), a_2(32),\ldots, a_{32}(32), b_1(32), b_2(32),\ldots., b_{32}(32))$.

Chú ý : các S-box có thể được sử dụng làm khóa thời gian dài.

3.6 Bộ luật Liên Bang Nga về chữ ký số

Chương 1. Các điều khoản chung

Điều 1.Mục đích và phạm vi áp dụng bộ luật Liên Bang này

1. Đảm bảo điều kiện luật pháp cho việc sử dụng chữ ký điện tử số là mục đích của bộ luật Liên Bang này, theo nó thì chữ ký điện tử số trong các văn bản điện tử được công nhận có giá trị như chữ ký bằng tay trên văn bẳn giấy tờ.

2. Hiệu lực của bộ luật Liên Bang này được áp dụng cho các quan hệ được xuất hiện khi tiến hành các hợp đồng pháp lý dân sự và trong các trường hợp khác được xem trước bằng luật pháp của Liên Bang Nga.

Hiệu lực của bộ luật Liên Bang này không áp dụng cho các quan hệ được xuất hiện khi sử dụng các tương tự khác của chữ ký tay.

Điều 2. Điều chỉnh pháp quyền các quan hệ trong lĩnh vực sử dụng chữ ký điện tử số.

Điều chỉnh pháp quyền các quan hệ trong lĩnh vực sử dụng chữ ký điện tử số được thực hiện theo bộ luật Liên Bang này, bộ luật dân sự của Liên Bang Nga, luật Liên Bang "Về thông tin, thông tin hóa vá các bảo vệ thông tin", Luật Liên Bang "Về thông tin", và các luật Liên Bang khác và các văn bản pháp luật pháp chuẩn của Liên Bang Nga đã được áp dụng theo các bộ luật đã nêu, và cũng được thực hiện theo thoả thuận của các bên.

Điều 3. Các khái niệm cơ bản được sử dụng trong bộ luật Liên Bang này

Vì các mục đích của bộ luật Liên Bang này, các khái niệm cơ bản sau được sử dụng :

Văn bản điện tử - đó là văn bản, trong đó thông tin được biểu diễn ở dạng điện tử số.

Chữ ký điện tử số - phụ lục của một văn bản điện tử, dùng để bảo vệ văn bản điện tử đó khỏi giả mạo, nhận được như kết quả của phép biến đổi mật mã đối với thông tin với việc sử dụng khóa bí mật của chữ ký điện tử số và cho phép nhận dạng người chủ của chứng nhận khóa chữ ký, đồng thời cũng khẳng định việc thông tin trong văn bản điện tử không bị xuyên tạc.

Người chủ của giấy chứng nhận khóa chữ ký - người được trung tâm chứng thực cấp cho giấy chứng nhận khóa ký và nắm giữ khóa bí mật tương ứng của chữ ký điện tử số, khóa bí mật này cho phép với sự giúp đỡ của các phương tiện chữ ký điện tử tạo ra chữ ký điện tử số của người đó trong các văn bản điện tử (ký các văn bản điện tử).

Các phương tiện chữ ký điện tử - các công cụ máy móc hay phần mềm, đảm bảo việc thực hiện một trong các chức năng sau: tạo chữ ký điện tử số trong các văn bản điện tử với việc sử dụng khóa bí mật của chữ ký điện tử số, khẳng định tính chân thực của chữ ký điện tử số trong các văn bản điện tử bằng việc sử dụng khóa bí mật của chữ ký điện tử số, tạo ra các khóa bí mật và công khai của chữ ký điện tử số.

Giấy chứng nhận của các phương tiện chữ ký điện tử số văn bản trên giấy được cấp theo các quy định của hệ thống chứng thực để khẳng định tính tuân thủ các yêu cầu đã được thiết lập của các phương tiện chữ ký điện tử số.

Khóa bí mật của chữ ký điện tử số dãy duy nhất các ký hiệu, được biết bởi người chủ của chứng nhận khóa chữ ký và dùng để tạo ra chữ ký điện tử số trong các văn bản điện tử bằng việc dùng các phương tiện chữ ký điện tử số.

Khóa công khai chữ ký điện tử số - dãy duy nhất các ký hiệu, tương ứng với khóa bí mật chữ ký điện tử số, được biết bởi một người sử dụng bất kỳ của hệ thống thông tin và được dùng để khẳng định tính chân thực của chữ ký điện tử số trong văn bản điện tử bằng cách sử dụng các phương tiện chữ ký điện tử số.

Giấy chứng nhận khóa chữ ký văn bản trên giấy hoặc văn bản điện tử cùng với chữ ký điện tử số của người có trách nhiệm thuộc trung tâm chứng thực, trong đó có khóa công khai của chữ ký điện tử số, và được trung tâm chứng thực cấp cho người tham gia hệ thống thông tin để khẳng định tính chân thực của chữ ký điện tử số và nhận dạng người chủ của chứng nhận khóa chữ ký.

Khẳng định tính chân thực của chữ ký điện tử số trong văn bản điện tử kết quả tán thành của việc kiểm tra bằng các phương tiện chứng thực tương ứng chữ ký điện tử số cùng với việc sử dụng chứng nhận khóa chữ ký tính phụ thuộc của chữ ký điện tử số vào người chủ của chứng nhận khóa chữ ký và tính thiếu vắng sự thay đổi trong văn bản điện tử bởi chữ ký điện tử số đã cho.

Người sử dụng chứng nhận khóa chữ ký - người sử dụng các thông tin nhận được tại trung tâm chứng thực về giấy chứng nhận khóa chữ ký để kiểm tra tính phụ thuộc của chữ ký điện tử số với chủ chứng nhận khóa chữ ký.

Hệ thống thông tin doanh nghiệp - hệ thống thông tin mà những người tham gia là một nhóm người giới hạn, được xác định bởi người chủ của hệ thống hoặc bằng thỏa thuận của những người tham gia hệ thống thông tin này.

Chương II. Các điều kiện sử dụng chữ ký điện tử số

Điều 4. Các điều kiện để công nhận giá trị như nhau của chữ ký điện tử số và chữ ký viết tay

1. Chữ ký điện tử số trong văn bản điện tử có giá trị như chữ ký viết tay trong văn bản trên giấy nếu như đồng thời tuân thủ các điều kiện sau:

Chứng nhận khóa chữ ký thuộc về chữ ký điện tử số này không mất hiệu lực (còn tác dụng) tại thời điểm kiểm tra hoặc thời điểm ký văn bản điện tử nếu như có bằng chứng xác định thời điểm ký;

Tính chân thực của chữ ký trong văn bản điện tử được khẳng định.

Chữ ký điện tử số được sử dụng theo như những quy định được chỉ ra trong giấy chứng nhận khóa chữ ký.

2. Người tham gia hệ thống thông tin có thể đồng thời là chủ của một số lượng bất kỳ giấy chứng nhận khóa chữ ký. Khi đó văn bản điện tử cùng với chữ ký điện tử số có giá trị pháp lý khi thực hiện các quan hệ được chỉ ra trong giấy chứng nhận khóa chữ ký.

Điều 5. Sử dụng các phương tiện chữ ký điện tử số

1. Việc sinh các khóa chữ ký điện tử số được thực hiện để sử dụng trong :

Hệ thống thông tin sử dụng chung bởi người tham gia hệ thống hay bởi trung tâm chứng thực theo yêu cầu của người tham gia.

Hệ thống thông tin doanh nghiệp theo quy cách được thiết lập trong hệ thống đó.

2. Khi sinh khóa chữ ký điện tử số để sử dụng trong hệ thống thông tin sử dụng chung cần phải chỉ áp dụng các phương tiện đã được cấp phép chữ ký điện tử số. Việc đền bù thiệt hại gây ra do sinh khóa chữ ký điện tử số bởi các phương tiện chữ ký điện tử số không được cấp phép có thể quy trách nhiệm cho những người tạo ra và những người phân phối các phương tiện này theo như pháp luật Liên Bang Nga.

3. Việc sử dụng các phương tiện chữ ký điện tử số không được cấp phép và các chữ ký điện tử số được sinh ra bởi chúng trong các hệ thống thông tin doanh nghiệp của các cơ quan Liên Bang thuộc chính quyền quốc gia, các cơ quan chính quyền quốc gia của các chủ thể Liên Bang Nga và các cơ quan điều hành địa phương là không được phép.

4. Việc cấp phép các phương tiện chữ ký điện tử số được thực hiện theo pháp luật pháp Liên Bang Nga về cấp phép sản phẩm và dịch vụ.

Điều 6. Chứng nhận khóa chữ ký

1. Chứng nhận khóa chữ ký cần chứa các thông tin sau:

Số đăng ký duy nhất của chứng nhận khóa chữ ký, ngày bắt đầu và kết thúc thời hạn hiệu lực của chứng nhận chữ ký số nằm ở danh sách của trung tâm chứng thực.

Họ tên và tên đệm của người chủ chứng nhận khóa chữ ký hay bí danh của người chủ. Trong trường hợp sử dụng bí danh, trung tâm chứng thực cần ghi điều đó vào chứng nhận khóa chữ ký.

Khóa công khai của chữ ký điện tử số.

Tên của các phương tiện chữ ký điện tử số, mà khóa công khai của chữ ký điện tử số này được sử dụng với. Tên và địa điểm của trung tâm chứng thực cấp ra chứng nhận khóa chữ ký.

Các chỉ dẫn về các quan hệ mà khi thực hiện nó thì văn bản điện tử với chữ ký điện tử số sẽ có giá trị pháp lý.

2. Trong trường hợp cần thiết, trong chứng thực nhận khóa chữ ký, trên cơ sở các văn bản đã được xác nhận còn chỉ ra chức vụ (cùng với tên và địa điểm của cơ quan đã lập ra chức danh đó) và nghề nghiệp của chủ chứng nhận khóa chữ ký, còn theo sự xuất trình ở dạng viết những tư liệu khác đã được xác nhận bởi các giấy tờ khác.

3. Chứng nhận khóa chữ ký cần phải được trung tâm chứng thực đưa vào danh sách của các chứng nhận khóa chữ ký không muộn hơn ngày bắt đầu có hiệu lực của chứng nhận khóa chữ ký.

4. Để kiểm tra tính sở hữu chữ ký điện tử số với người chủ chứng nhận khóa chữ ký, những người sử dụng được trao thông tin về ngày và thời gian cấp chứng nhận, tư liệu về hiệu lực của chứng nhận khóa chữ ký (có hiệu lực, dừng có hiệu lực, thời hạn dừng có hiệu lực, đã bị hủy bỏ, ngày và thời gian hủy bỏ chứng nhận chữ ký) và tư liệu về danh sách của chứng nhận khóa chữ ký. Trong

trường hợp cấp chứng nhận khóa chữ ký ở dạng văn bản trên giấy, chứng nhận này được thể hiện theo khuôn mẫu của trung tâm chứng thực và được làm tin bởi chữ ký tay của người có chức trách và dấu của trung tâm chứng thực.Trong trường hợp cấp chứng nhận khóa chữ ký và các dữ liệu bổ sung đã nêu ở dạng văn bản điện tử, chứng nhận đó cần phải được ký bởi chữ ký điện tử số của người có trách nhiệm thuộc trung tâm chứng thực.

Điều 7. Thời hạn và cách thức lưu giữ chứng nhận khóa chữ ký tại trung tâm chứng thực

1. Thời hạn lưu giữ chứng nhận khóa chữ ký ở dạng văn bản điện tử tại trung tâm chứng thực được xác định bằng thỏa thuận giữa trung tâm chứng thực và người chủ của chứng nhận khóa chữ ký. Khi đó đảm bảo quyền truy cập của những người tham gia hệ thống thông tin vào trung tâm chứng thực để nhận được chứng nhận khóa chữ ký.

2. Thời hạn lưu giữ chứng nhận khóa chữ ký ở dạng văn bản điện tử tại trung tâm chứng thực sau khi hủy bỏ chứng nhận khóa chữ ký cần không được ít hơn thời hạn được thiết lập bởi luật Liên Bang về thời hạn kiện tụng đối với các quan hệ khi hết thời hạn lưu trữ đã chỉ ra, chứng nhận khóa chữ ký được loại bỏ khỏi danh sách của các chứng nhận khóa chữ ký và được đưa vào chế độ lưu trữ.

Thời hạn lưu không ít hơn 5 năm, Quy tắc đưa bản sao của chứng nhận khóa chữ ký trong giai đoạn này được thiết lập theo như luật pháp Liên Bang Nga.

3. Chứng nhận khóa chữ ký ở dạng văn bản trên giấy được lưu trữ theo quy định được thiết lập theo luật pháp Liên Bang Nga về văn khố và lưu trữ.

Chương III. Các trung tâm chứng thực

Điều 8. Vị trí của trung tâm chứng thực

1. Cơ quan luật pháp thực hiện các chức năng được xem xét bởi luật Liên Bang này là trung tâm chứng thực cấp các chứng nhận khóa chữ ký số để sử dụng trong các hệ thống thông tin dùng chung. Khi đó, trung tâm chứng thực cần phải có các khả năng tài chính và vật chất cần thiết, cho phép nó thi hành

trách nhiệm dân sự trước những người sử dụng khóa cũ ký đối với những thiệt hại.

Điều 10. Quan hệ giữa các trung tâm chứng thực và các cơ quan toàn quyền Liên Bang của chính quyền hành pháp

1. Trung tâm chứng thực cho đến khi bắt đầu sử dụng chữ ký điện tử số của người đại diện trung tâm chứng thực để cam đoan thay mặt trung tâm chứng thực các chứng nhận khóa chữ ký nhất định phải trình tại cơ quan đại diện Liên Bang của chính quyền hành pháp chứng thực của người đại diện trung tâm chứng thực ở dạng văn bản điện tử cũng như chứng nhận này ở dạng văn bản trên giấy cùng với chữ ký tay của người đại diện đã nêu, được cam đoan bởi chữ ký của người lãnh đạo và dấu của trung tâm chứng thực.

2. Cơ quan đại diện Liên Bang của chính quyền hành pháp thực hiện một danh sách quốc gia duy nhất các chứng nhận khóa chữ ký được đưa ra bởi các trung tâm chứng thực làm việc với những người tham gia hệ thống thông tin dùng chung (các trung tâm này cam đoan về những chứng nhận khóa chữ ký do mình đưa ra), đảm bảo khả năng truy nhập tự do tới danh sách này và cấp các chứng nhận khóa chữ ký cho những đại diện tương ứng của các trung tâm chứng thực.

3. Các chữ ký điện tử số của những người đại diện các trung tâm chứng thực có thể được sử dụng chỉ sau khi đưa nó vào một danh sách hợp nhất toàn quốc gia gồm các chứng nhận khóa chữ ký. Việc sử dụng các chữ ký điện tử này vào các mục đích không liên quan đến việc cam kết các chứng nhận khóa chữ ký cả các tư liệu về hiệu lực của nó là không cho phép.

4. Cơ quan đại diện Liên Bang của chính quyền hành pháp:

Thực hiện theo yêu cầu của mọi người, tổ chức, cơ quan Liên Bang của chính quyền hành pháp, các cơ quan chính quyền quốc gia của các chủ thể thuộc Liên Bang Nga và các cơ quan tự điều hành địa phương việc khẳng định tính đúng đắn của chữ ký điện tử số của các đại diện trung tâm chứng thực trong các chứng nhận khóa chữ ký do họ cấp phát.

Thực hiện theo các điều khoản về cơ quan đại diện Liên Bang của chính quyền lập pháp các ủy quyền khác để đảm bảo hiệu lực của bộ luật Liên Bang này.

Điều 11. Các trách nhiệm của trung tâm chứng thực trong quan hệ với người chủ chứng nhận khóa chữ ký

Trung tâm chứng thực chuẩn bị chứng nhận khóa chữ ký nhận về mình các trách nhiệm sau theo quan hệ với người chủ chứng nhận khóa ký.

Đưa chứng nhận khóa chữ ký vào danh sách chứng nhận khóa chữ ký.

Đảm bảo việc cung cấp chứng nhận khóa chữ ký cho những người tham gia hệ thống thông tin yêu cầu.

Dừng hiệu lực của chứng nhận khóa chữ ký theo yêu cầu người chủ của nó.

Thông báo cho người chủ chứng nhận khóa chữ ký về các sự kiện được biết bởi trung tâm chứng thực và bằng một cách nào đó có thể ảnh hưởng đến khả năng sử dụng tiếp theo của chứng nhận khóa chữ ký.

Các trách nhiệm khác được thiết lập bằng các điều khoản luật chuẩn mực hoặc thỏa thuận các bên.

Điều 12. Các trách nhiệm của người chủ chứng nhận khóa chữ ký

1. Người chủ của chứng nhận khóa chữ ký phải :

Không sử dụng cho chữ ký điện tử số các khóa công khai và bí mật của chữ ký điện tử số nếu như biết rằng các khóa đó đang sử dụng hoặc đã sử dụng;

Giữ bí mật khóa mật của chữ ký điện tử số.

Ngay lập tức yêu cầu dừng hiệu lực của chứng nhận khóa chữ ký khi có cơ sở cho rằng bí mật đối với khóa mật chữ ký điện tử số bị vi phạm.

2. Khi không tuân thủ những yêu cầu được nêu ra trong điều này, việc đền bù những thiệt hại gây ra do nó được gán cho trách nhiệm của người chủ chứng nhận khóa chữ ký.

Điều 13. Chấm dứt hiệu lực của chứng nhận khóa chữ ký

1. Hiệu lực của chứng nhận khóa chữ ký có thể bị dừng bởi trung tâm chứng thực trên cơ sở chỉ ra người hay cơ quan có quyền như vậy theo quy luật hay

thỏa ước, còn trong hệ thống thông tin doanh nghiệp còn theo như các quy tắc đã được thiết lập để sử dụng nó.

2. Thời gian từ lúc nhận được tại trung tâm chứng thực thực hiện lệnh về việc dừng hiệu lực của chứng nhận khóa chữ ký cho đến khi đưa thông tin tương ứng vào danh sách chứng nhận khóa chữ ký cần được thiết lập theo quy tắc chung đối với tất cả những người chủ chứng nhận khóa chữ ký.

3. Hiệu lực của chứng nhận khóa chữ ký theo lệnh của người (cơ quan) đại diện toàn quyền được dùng lại trong một thời hạn đươc tính theo ngày nếu hiệu lực đó không được thiết lập bởi các quy định luật chuẩn tắc hoặc thỏa ước. trung tâm chứng thực khôi phục hiệu lực của chứng nhận khóa chữ ký theo lệnh của người (cơ quan) đại diện toàn quyền. Trong trường hợp, nếu đã hết hạn chỉ ra mà không có lệnh về việc khôi phục hiệu lực của chứng nhận khóa chữ ký thì chứng nhận đó bị hủy bỏ.

4. Theo lệnh của người (cơ quan) đại diện về dừng hiệu lực của chứng nhận khóa chữ ký, trung tâm chứng thực loan báo điều này cho mọi người sử dụng chứng nhận tin tương ứng chỉ ra ngày, thời gian và thời hạn dừng hiệu lực của chứng nhận khóa chữ ký, đồng thời thông báo cho người chủ chứng nhận khóa chữ ký và người dùng (cơ quan) đại diện ra lệnh dừng hiệu lực của chứng nhận khóa chữ ký.

Điều 14. Hủy bỏ chứng nhận khóa chữ ký

1. Trung tâm chứng thực, nơi đã cấp chứng nhận khóa chữ ký, bắt buộc phải hủy bỏ nó:

Khi hết thời hạn có hiệu lực.

Khi bị mất sức mạnh pháp lý về chứng nhận của các phương tiện tương ứng của chữ ký điện tử số được sử dụng trong các hệ thống dùng chung.

Trong trường hợp nếu trung tâm chứng thực biết chắc chắn việc dừng hiệu lực của văn bản trên cơ sở đó lập ra chứng nhận khóa chữ ký.

Trong các trường hợp khác được thiếp lập bởi các điều luật chuẩn hoặc thỏa thuận giữa các bên.

2. Trong trường hợp hủy bỏ chứng nhận khóa chữ ký, trung tâm chứng nhận khóa chữ ký, trung tâm chứng thực thông báo về việc đó đến mọi người sử dụng chứng nhận khóa chữ ký bằng cách đưa vào danh sách các chứng nhận khóa chữ ký thông tin tương ứng cùng với việc chỉ ra ngày, giờ hủy bỏ chứng nhận khóa chữ ký, trừ trường hợp hủy bỏ chứng nhận khóa chữ ký khi hết thời hạn hiệu lực của nó đồng thời cũng thông báo điều này cho người chủ chứng nhận khóa chữ ký và người (cơ quan) đại diện đã ra lệnh hủy bỏ chứng nhận khóa chữ ký.

Điều 15. Chấm dứt hoạt động của trung tâm chứng thực

1. Hoạt động của trung tâm chứng thực nơi cấp chứng nhận khóa chữ ký để sử dụng trong các hệ thống thông tin dùng chung, có thể được dùng lại theo quy tắc được thiết lập bởi luật dân sự.

2. Trong trường hợp dừng hoạt động của trung tâm chứng thực đã được chỉ ra ở điểm 1 của điều này, các chứng nhận khóa chữ ký được cấp bởi trung tâm chứng thực đó, có thể được chuyển giao cho một trung tâm chứng thực khác theo thỏa thuận với những người chủ chứng nhận khóa chữ ký.

Các chứng nhận khóa chữ ký không được chuyển cho một trung tâm chứng thực khác, được hủy bỏ và chuyển cơ quan toàn quyền Liên Bang để đưa vào lưu trữ theo điều 7 của luật Liên Bang này.

1. Hoạt động của trung tâm chứng thực đảm bảo hoạt động của hệ thống thông tin doanh nghiệp được dùng theo quyết định của người chủ hệ thống đó, đồng thời cũng theo thỏa thuận của những người tham gia hệ thống nếu có sự chuyển giao trách nhiệm của trung tâm này cho một trung tâm khác hoặc khi xóa bỏ hệ thống thông tin doanh nghiệp.

Chương IV. Các đặc điểm sử dụng chữ ký điện tử số

Điều 16. Sử dụng chữ ký điện tử số trong lĩnh vực điều hành Nhà Nước

1. Các cơ quan Liên Bang của chính quyền hành pháp, các cơ quan chính quyền Quốc Gia của các chủ thể trong Liên Bang Nga, các cơ quan tự điều hành đã nêu trên sử dụng các chữ ký điện tử số của những người lãnh đạo các cơ quan, tổ chức đó để ký các văn bản điện tử của mình.

2. Các chứng thực khóa chữ ký của những người đại diện toàn quyền các cơ quan Liên Bang của chính quyền quốc gia được đưa vào danh sách các chứng nhận khóa chữ ký được quản lý bởi cơ quan đại diện Liên Bang của chính quyền hành pháp, và được cấp phát cho những người sử dụng chứng nhận khóa chữ ký từ danh sách này theo quy định được thiết lập bởi bộ luật Liên Bang này cho các trung tâm chứng thực.

3. Quy tắc cấp chứng nhận khóa chữ ký của những người đại diện các cơ quan chính quyền quốc gia của các chủ thể trong Liên Bang Nga và những người đại diện các cơ quan tự điều hành địa phương được thiết lập bởi các điều luật chuẩn tắc của cơ quan tương ứng.

Điều 17. Sử dụng chữ ký số trong hệ thống thông tin doanh nghiệp

1. Hệ thống thông tin doanh nghiệp cung cấp cho những người tham gia hệ thống thông tin sử dụng các dịch vụ của trung tâm chứng thực của hệ thống thông tin doanh nghiệp cần phải đáp ứng được các yêu cầu được quy định bởi bộ luật Liên Bang này cho các hệ thống thông tin dùng chung.

2. Quy tắc sử dụng chữ ký điện tử số trong hệ thống tin doanh nghiệp được thiết lập bởi quyết định của người chủ hệ thống đó hay bởi thỏa thuận của những người tham gia hệ thống.

3. Nội dung thông tin trong các chứng nhận khóa chữ ký, quy tắc đưa vào danh sách các chứng nhận khóa chữ ký ấy đã đăng ký, quy định lưu giữ các chứng nhận khóa chữ ký đã được hủy bỏ, các trường hợp mất hiệu lực pháp lý của các chứng nhận đã nêu ra trong hệ thống thông tin doanh nghiệp được thể chế hóa bằng quyết định của người chủ hệ thống hay bởi thỏa thuận của những người tham gia hệ thống thông tin doanh nghiệp.

Điều 18. Công nhận chứng nhận khóa chữ ký của nước ngoài

Chứng nhận khóa chữ ký của nước ngoài, được chứng thực theo như luật pháp của nước mà chứng nhận khóa chữ ký ấy đã đăng ký, được công nhận trên lãnh thổ Liên Bang Nga trong các trường hợp thực hiện các qui trình được thiết

lập bởi luật pháp Liên Bang Nga về việc công nhận giá trị pháp lý của các văn bản nước ngoài.

Điều 19. Các trường hợp thay thế con dấu

1. Nội dung văn bản trên giấy, được đảm bảo bởi con dấu và được chuyển thành văn bản điện tử, theo như các điều luật chuẩn hoặc thỏa thuận giữa các bên có thể được đảm bảo bằng chữ ký điện tử số của người đại diện cơ quan có con dấu.

2. Trong các trường hợp được quy định bởi luật hoặc các điều luật chuẩn khác của Liên Bang Nga hoặc thỏa thuận giữa các bên, chữ ký điện tử số trong văn bản điện tử, chứng nhận của nó chứa các tư liệu cần thiết để thực hiện các quan hệ đang xét đến về quyền lực của người chủ, được công nhận có giá trị như chữ ký tay của người trên văn bản bằng giấy được đảm bảo bằng con dấu.

Chương V. Các điều khoản thi hành và chuyển giao

Điều 20. Thi hành các văn bản pháp lý chuẩn mực theo như luật Liên Bang này.

1. Các điều luật chuẩn của Liên Bang Nga được đưa vào hoạt động theo như luật Liên Bang này trong vòng 3 tháng kể từ ngày luật Liên Bang này có hiệu lực.

2. Các văn bản hành chính của các trung tâm chứng thực, nơi cấp các chứng nhận khóa chữ ký để sử dụng trong các hệ thống thông tin dùng chung, được đưa vào hoạt động theo luật Liên Bang này trong vòng 6 tháng kể từ ngày có hiệu lực.

Điều 21. Các điều khoản chuyển giao.

Các trung tâm chứng thực được thành lập sau ngày luật Liên Bang này có hiệu lực, trước khi được cơ quan đại diện Liên Bang của chính quyền hành pháp đưa vào danh sách các chứng nhận khóa chữ ký cần phải đáp ứng yêu cầu của luật Liên Bang này, ngoại trừ yêu cầu xuất trình trước đó các chứng nhận khóa chữ ký của cả người đại diện nhà nước mình trước các cơ quan đại diện Liên Bang của chính quyền hành pháp. Các chứng nhận tương ứng cần phải trình cho

các cơ quan tương ứng không chậm hơn 3 tháng sau kể từ ngày có hiệu lực của luật Liên Bang này.

3.7 So sánh GOST 28147 -89 với thuật toán Rijndael

Ngày 2 tháng 10 năm 2000, bộ thương mại Mỹ đã tổng kết cuộc thi tuyển chọn thuật toán mã hóa mới của nước Mỹ. Người chiến thắng là thuật toán Rijndael. Thuật toán mã hóa mới này được thay thế cho DES, đó là chuẩn mã hóa của Mỹ từ năm 1977.

DES được thiết kế tại phòng nghiêm cứu của hãng IBM vào nửa đầu những năm 70 của thế kỷ 20 và thuộc về họ các mã pháp khởi nguồn từ thuật toán Lucifer cũng được nghiêm cứu tại nơi đó một số năm trước. Kiến trúc này, có tên gọi là mạng Feistel có vị trí quan trọng trong mật mã học cho đến ngày hôm nay: phần lớn các mã pháp hiện đại đều có dạng này, trong đó có cả chuẩn mã của Nga GOST 28147 - 89. Ta sẽ phân tích so sánh GOST 28147 - 89 với Rijndael, trên cơ sở đó tiến hành việc so sánh phương pháp cổ điển và hiện đại trong việc xây dựng mã khối.

Chỉ tiêu	Gost 28147-89	Rijndael
Kích thước khối, bit	64	128, 192,256
Kích thước khóa, bit	256	128, 192, 256
Kiến trúc	Mạng cân bằng Feistel	Hình vuông
Số vòng	32	10, 12, 14
Phần của khối rõ được mã sau mỗi vòng	Nửa khối(32 bit)	Cả khối (128, 192, 256)
Kích thước của khóa vòng, bit	Nửa độ dài khối	Bằng độ dài khối
Cấu trúc vòng	Đơn giản	Tương đối phức tạp
Các phép toán được sử dụng	Chỉ có phép cộng, thay thế, và phép dịch	Sử dụng rộng rãi các phép toán trên trường hữu hạn
Tính tương đương của biến đổi thuận nghịch	Chính xác đến thứ tự của các khóa vòng	Chính xác đến vecto của các phần tử khóa, bảng các thay thế và hằng số của thuật toán

So sánh các đặc tính chung của 2 thuật toán

Các đặc tính so sánh của thuật toán GOST 28147 - 89 với Rijndael đã chỉ ra bảng trên. Khác với thuật toán của Nga, kích thước khóa trong thuật toán Rijndael có thể thay đổi, điều này do sử dụng cấu trúc "hình vuông", tính chất này cho phép thay đổi độ bền vững cũng như tốc độ thực hiện thuật toán theo sự phụ thuộc vào các yếu tố bên ngoài khi cần cài đặt trong một giới hạn nhất định, tuy nhiên không rộng lắm, đó là số các vòng, và cùng với nó là tốc độ trong các trường hợp khác biệt nhau nhất vào khoảng 1,4 lần.

So sánh các nguyên tắc chung

Việc phân tích thuật toán GOST 28147 - 89 cũng như phần lớn các mã pháp thuộc thế hệ đầu tiên được thiết kế vào những năm 70 và nửa đầu những năm

80, được dựa trên kiến trúc mạng Feistel cân bằng. Nguyên tắc chính của kiến trúc này là cả quá trình mã gồm một loạt các vòng có kiểu giống nhau. Tại mỗi vòng, khối được mã T được chia thành hai nửa (T_o, T_1), một trong chúng được thay đổi bằng phép cộng modulo 2 theo từng bit với giá trị được làm ra từ phần còn lại và bộ phận khóa vòng với sự giúp đỡ của hàm mã. Giữa các vòng, hai phần của khối đổi chỗ cho nhau, như vậy tại vòng sau, phần của khối thay đổi ở vòng trước sẽ không thay đổi và ngược lại. Lược đồ thuật toán GOST 28174 - 89 hình 1(a). Kiến trúc như vậy cho phép dễ dàng nhận được phép giải mã từ một hàm mã phức tạp, và có thể là không có ngược. Đặc tính quan trọng của phương pháp này là tại mỗi vòng chỉ mã đúng một nửa khối.

T, T’ -khối rõ và khối mã

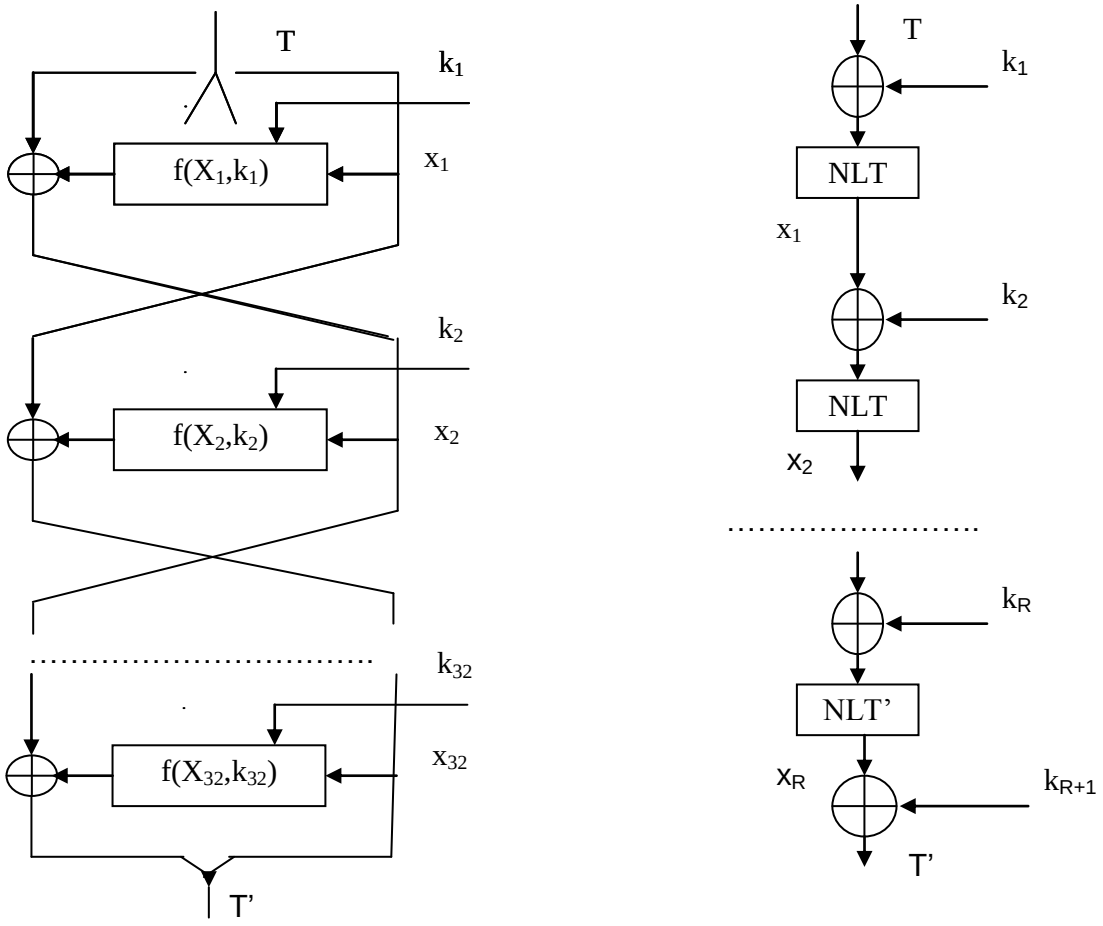
k_i -thành phần khóa vòng

X_i -trạng thái của quá trình mã sau mỗi vòng thứ i

f(X,k) -hàm mã của thuật toán GOST

NLT, NLT’ -biến đổi phi tuyến thông thường và biến đổi phi tuyến cho vòng cuối cùng của thuật toán Rijndael

R -số vòng của Rijndael (10, 12, hay 14)



a) b)

Hình 1. Lược đồ biến đổi dữ liệu khi mã
theo thuật toán GOST a) và Rijndael b)

Mã Rijndael có một kiến trúc khác về mặt nguyên tắc, nó được gọi là " Hình vuông" theo tên của mã pháp đầu tiên có cấu trúc kiểu này cũng do chính các tác giả của Rijndael thiết kế ra một số năm trước đây. Kiến trúc này dựa trên các biến đổi trực tiếp khối được mã khi được biểu diễn ở dạng ma trận của các byte. Việc mã cũng gồm một loạt các bước có kiểu giống nhau, đó là các vòng, nhưng tại mỗi vòng cả khối đều được biến đổi chứ không có phần nào của khối được giữ nguyên. Như vậy, sau một vòng cả khối được mã, cho nên để đảm bảo độ phức tạp tương ứng và tính phi tuyến của biến đổi, số các bước yêu cầu như vậy sẽ ít hơn 2 lần so với cấu trúc Feistel. Mỗi vòng bao gồm từng bit theo modulo 2 giữa trạng thái hiện tại của khối được mã và thành phần khóa vòng, sau đó là một phép biến đổi phi tuyến phức tạp của cả khối, biến đổi phi tuyến này được

kiến thiết từ 3 biến đổi đơn giản hơn sẽ được xem xét chi tiết ở phần sau. Lược đồ của mã Rijndael được đưa ra ở hình 1(b).

So sánh các vòng mã trong thuật toán GOST sử dụng hàm mã tương đối không phức tạp, gồm có phép cộng của nửa khối vào với thành phần khóa vòng tương ứng theo modulo 2^{32}, 8 phép thay thế thực hiện một cách độc lập trong các nhóm 4 bit và phép hoán vị bit (quay 11 bit về phía hàng cao). Lược đồ phép mã này ở hình 2(a).

Trong thuật toán Rijndael, khối được mã và các trạng thái trung gian của nó trong quá trình biến đổi được biểu diễn ở dạng ma trận 4 x n byte, với n = 4, 6, 8 tùy thuộc vào kích thước khối. Hàm biến đổi phi tuyến trong thuật toán Rijndael bao gồm 3 phép biến đổi đơn giản sau thực hiện lần lượt:

- Thay thế byte - mỗi byte của khối được biến đổi được thay bằng giá trị mới, lấy từ một vecto thay thế chung cho tất cả các byte của ma trận.
- Phép dịch vòng theo byte trong các dòng của ma trận: dòng đầu tiên không đổi, dòng thứ 2 dịch vòng về phía trái một byte, dòng thứ 3, 4 dịch về phía bên trái tương ứng 2 hay 3 byte ứng với n=4,6; còn với n=8 ứng với 3 hay 4 byte.
- Nhân ma trận - ma trận được nhận ở bước trên nhân trái với ma trận hồi chuyển kích cỡ 4x4:

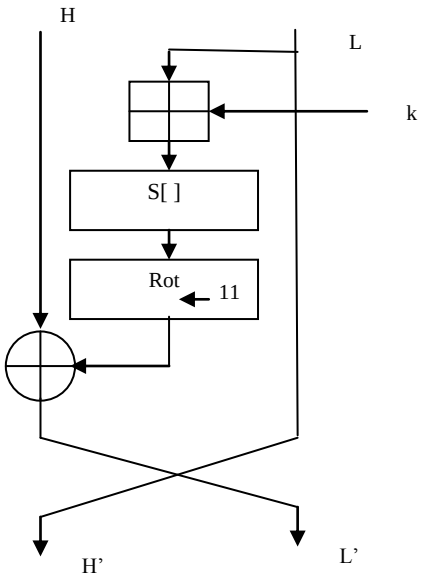
$$M=\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Các phần tử của ma trận được xem như là các phần tử của trường hữu hạn GF(2^8), tức là các đa thức có bậc không quá 7, hệ số của chúng là các bit, các phép cộng và nhân theo mudolo 2. Trong trường hữu hạn này, phép cộng các

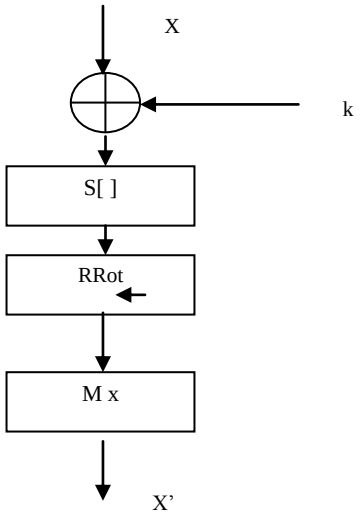
byte như là phép cộng từng bit theo modulo 2, còn phép nhân được lấy theo modulo của đa thức bất khả qui

$x^8+x^4+x^3+x+1$ với các hệ số từ GF(2). Lược đồ vòng của thuật toán Rijndael biểu diễn ở hình 2(b).

Nếu trong thuật toán GOST phép hoán vị 2 nửa khối được đưa vào các vòng mã như chỉ ra ở hình 2(a), thì có thể nhận thấy rằng trong cả 2 thuật toán, các vòng mã luôn giống nhau, trừ vòng cuối cùng, tại đó thiếu một phần phép toán. Cách như vậy cho phép nhận được một cách thể hiện gọn ghẽ hơn, cả trong thiết bị lẫn lập trình. Tại vòng cuối cùng GOST không có phép hoán vị 2 nửa khối đã được mã, còn đối với Rijndael là phép nhân bên trái với ma trận M. Trong cả hai thuật toán được bàn đến, điều này đảm bảo tính tương đương cấu trúc của biến đổi mã và giải mã.



a)



b)

X, X' – khối được biến đổi ở đầu vào và ra của vòng

(H, L), (H', L') – phần cao và phần thấp ở đầu vào và ra của vòng

k – khóa vòng

S[ ] – hàm thay thế, được nhóm theo 4 bit cho GOST và của các byte cho Rijndael

Rot←11 – phép quay từ 32 bit về phía bit cao 11 lần

Rrot – phép toán quay ma trận theo dòng của thuật toán Rijndael

Mx – ma trận M trong thuật toán Rijndael với ma trận dữ liệu ở bên trái

Tính tương đương của biến đổi ngược và xuôi

Trong thuật toán GOST tính tương đương cấu trúc của biến đổi xuôi và ngược không đảm bảo một cách đặc biệt mà là hệ quả đơn giản của việc áp dụng giải pháp kiến trúc. Trong một mạng cân bằng Feistel bất kỳ, hai biến đổi này tương đương và chỉ khác nhau thứ tự sử dụng với thứ tự ngược lại so với thứ tự được sử dụng lúc mã.

Thuật toán Rijndael được xây dựng trên cơ sở các biến đổi trực tiếp. Cũng như biến đổi với tất cả các thuật toán tương tự, biến đổi ngược được xây dựng từ việc đảo ngược các bước của biến đổi xuôi theo thứ tự ngược lại. Do đó, việc đảm bảo tính đồng nhất của biến đổi xuôi và ngược như trong cấu trúc Feistel là không thể đạt được. Tuy vậy, bằng một giải pháp kiến trúc đặc biệt cũng đạt được một mức độ gần tương ứng biến đổi xuôi và ngược là đồng nhất với sự chính xác đến hằng số được sử dụng trong chúng. Trong bảng 2 dẫn ra 2 vòng cuối của thuật toán Rijndael và phép đảo ngược hình thức của nó.

Bảng 2 Hai vòng của thuật toán Rijndael và phép đảo ngược hình thức của nó

Biến đổi xuôi	Biến đổi ngược
$X=X\oplus k_{R-1}$	$X=X\oplus k_{R+1}$
$X=S(X)$	$X=RRot\rightarrow(X)$
$X=RRot\leftarrow(X)$	$X=S^{-1}(x)$
$X=M \times X$	$X=X\oplus k_R$
$X=X\oplus k_R$	$X=M^{-1} \times X$
$X=S(x)$	$X=RRot\rightarrow(X)$
$X=RRot \leftarrow(X)$	$X=S^{-1}(X)$
$X=X\oplus k_{R+1}$	$X=X\oplus k_{R-1}$

Trước hết cần chú ý rằng phép toán thay thế theo từng byte(S) có tính giao hoán với phép dịch theo byte các dòng của ma trận:

$S^{-1}(RRot\rightarrow(X))=RRot\rightarrow(S^{-1}(X))$.

Ngoài ra, theo các quy tắc của đại số ma trận theo định luật kết hợp cũng có thể thay đổi thứ tự cộng từng bit theo modulo 2 của khóa và phép nhân ma trận:

$$M^{-1}x\ (X\oplus k_R)=(M^{-1}\ x\ X\ )\oplus\ (M^{-1}\ x\ k_R)$$

Áp dụng các thay đổi đã chỉ ra vào cột hai của bảng 2, chúng ta nhận được dãy phép toán sau trong hai vòng của phép biến đổi ngược (bảng 3)

Bảng 3 Hai vòng của thuật toán Rijndael và ngược của nó

Biến đổi xuôi	Biến đổi ngược
$X=X\oplus k_{R-1}$	$X=X\oplus k_{R+1}$
$X=S(X)$	$X=S^{-1}(x)$
$X=RRot\leftarrow(X)$	$X=RRot\rightarrow(X)$
$X=M\ x\ X$	$X=M^{-1}\ x\ X$
$X=X\oplus k_R$	$X=X(M^{-1}\oplus k_R)$
$X=S(x)$	$X=S^{-1}(X)$
$X=RRot\leftarrow(X)$	$X=RRot\rightarrow(X)$
$X=X\oplus k_{R+1}$	$X=X\oplus k_{R-1}$

Từ việc so sánh các cột của bảng 3 ta dễ thấy rằng, cấu trúc hoạt động của biến đổi xuôi và ngược giống nhau. Kết quả dễ dàng tổng quát hóa cho một số vòng bất kỳ. Như vậy, trong thuật toán Rijndael thủ tục mã và giải mã hoạt động như nhau và chỉ khác nhau ở các chi tiết sau:

- Trong biến đổi ngược sử dụng phép thế vecto, ngược về hoạt động với vecto thay thế biến đổi xuôi.
- Trong biến đổi ngược, số byte mà theo nó mỗi dòng của ma trận dữ liệu dịch đi trong phép toán dịch từng dòng theo byte khác đi so với biến đổi xuôi.
- Trong biến đổi ngược, tại bước nhân ma trận là ngược với cái được sử dụng trong biến đổi xuôi, đó là

$$M=\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 03B & 0D & 09 & 0E \end{bmatrix}$$

- Trong biến đổi ngược, các phần tử khóa được sử dụng theo thứ tự ngược lại, ngoài ra tất cả các phần tử trừ phần tử đầu tiên và cuối cùng cần phải nhân phía bên trái với ma trận M^{-1}.

Như vậy, tương tự như GOST, trong thuật toán Rijndael có thể trùng hợp việc thực hiện bằng chương trình cũng như bằng thiết bị.

Chuẩn bị khóa

Trong chuẩn mã của nước Nga, để tạo ta các phần tử khóa 32 bit từ khóa 256 bit một phương pháp đơn giản được áp dụng. Khóa được hiểu như một mảng gồm 8 phần tử khóa : $K=(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$.

Các phần tử này được sử dụng trong các vòng mã mỗi khóa được xem đến 3 lần theo thứ tự xuôi và một lần theo chiều ngược lại, cuối cùng là mỗi phần tử khóa được sử dụng đúng 4 lần. Trong bảng 4 chỉ ra thứ tự của vòng và phần tử khóa được sử dụng.

Vòng	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Phần tử khóa	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
Vòng	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Phần tử khóa	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_8	K_7	K_6	K_5	K_4	K_3	K_2	K_1

Bảng 4 thứ tự sử dụng các phần tử khóa trong vòng mã của GOST 28147 – 89

Trong thuật toán Rijndael sử dụng lược đồ phức tạp hơn một chút, có tính đến khả năng khác nhau về kích thước của khối mã và khóa. Tồn tại hai thuật toán để sinh ra dãy các phần tử khóa cho khóa kích thước 128/192 bit và cho khóa kích thước 256 bit, chúng tương đối giống nhau và chỉ khác nhau chút ít. Khóa và dãy khóa được biểu diễn chính bằng các từ của khóa cũng như trong GOST. Các từ sau của dãy khóa được chọn theo quan hệ đồng dư từng nhóm một, là bội của kích cỡ khóa. Từ 4 byte đầu tiên của nhóm như vậy được tạo bởi việc sử dụng một biến đổi phi tuyến đủ phức tạp, những từ còn lại theo một quan hệ tuyến tính đơn giản.

Như vậy thuật toán tạo dãy khóa trong mã Rijndael là phức tạp hơn so với trong GOST. Tuy vậy, nó cũng đủ đơn giản và hiệu quả và đóng góp đáng kể vào khối lượng tiêu tốn tính toán chung khi mã tốc độ mã cùng với việc tính các phần tử khóa chút ít nhỏ hơn tốc độ mã cùng với khóa đã được chuẩn bị từ trước.

Chọn các nút thay thế và các hằng số khác

Các phần tử khóa dùng trong thời gian dài (các nút thay thế) là những hằng số quan trọng nhất của GOST 28147 - 89. Chúng không được chỉ ra trong chuẩn mà được cung cấp bởi các tổ chức chuyên nghành đặc biệt, chuyển giao cho người sử dụng khóa mã này. Vì thế không đưa ra một tiêu chuẩn thiết kế nào cho các nút thay thế này. Từ những suy luận chung có thể nhận thấy rằng, trước hết các nút thay thế được chọn bằng việc sử dụng một trong những phương pháp thiết kế các nút, sau đó được đánh giá theo một số tiêu chuẩn, khi đó những nút không đủ tiêu chuẩn sẽ bị bỏ đi. Trong số các tiêu chuẩn đánh giá, có lẽ có mặt các tiêu chuẩn sau :

Độ phức tạp và tính phi tuyến của hàm bool mô tả các nút

Đặc tính vi phân của các nút thay thế

Đặc tính tuyến tính của các nút thay thế

Khác với những người tạo ra GOST 28147 - 89, các tác giả của mã pháp Rijndael không giấu các tiêu chuẩn thiết kế vecto thay thế. Khi thiết kế chúng,

bên cạnh các yêu cầu đơn giản như tính có ngược và tính đơn giản khi mô tả còn có những suy tính sau được để ý đến :

Cực tiểu hóa đặc tính tương quan lớn nhất theo giá trị giữa các tổ hợp tuyến tính của các bit vào và các bit ra

Cực tiểu hóa giá trị không tầm thường lớn nhất trong bảng EXOR

Độ phức tạp của biểu thức đại số mô tả nút trong GF(2)

Tính năng suất và độ tiện lợi khi thể hiện

Khi đánh giá tính hiệu quả đạt được đối với cài đặt thiết bị của mã pháp thì tiêu chuẩn chủ yếu là số lượng và độ phức tạp của các phép tính cơ sở cần phải thực hiện trong một vòng lặp và cả khả năng song song hóa thuật toán. Khi đánh giá tính hiệu quả của các cài đặt chương trình có thể thì mối quan tâm chính là việc cài đặt trên những nền tảng 32 bit, vì các máy tính 32 bit tại thời điểm hiện tại chiếm chủ yếu đến cộng đồng máy tính của loài người. Việc cài đặt trên các bộ vi xử lý 8 bit cũng cần chú ý, vì đó là công nghệ chủ yếu của thẻ thông minh. Các thiết bị tương tự có thể được sử dụng trong các hệ thống khác nhau thanh toán chuyển khoản, chúng ngày một trở nên phổ biến trên thế giới số người sử dụng các hệ thống như vậy trong thời gian cuối tăng với tốc độ lớn.

Chuẩn mã GOST 28147 -89 của nước Nga thuận tiện thể hiện trong thiết bị cũng như phần mềm. Với kích thước khối dữ liệu bằng 64, công việc chủ yếu được tiến hành với một nửa của khối này, đó là các từ 32 bit, điều này cho phép thể hiện hiệu quả chuẩn mã của nước Nga trên phần lớn các máy tính hiện đại.

GOST cũng có khả năng thực hiện hiệu quả trên các bộ vi xử lý 8 bít, bởi vì các phép tính cơ sở tạo nên nó có trong bộ lệnh của phần lớn các bộ điều khiển phổ dụng nhất. Khi đó phép cộng theo modulo 232 buộc phải chia ra một phép cộng không nhớ và phép cộng có nhớ, được thực hiện tuần tự. Tất cả các phép toán còn lại cũng có thể biểu diễn trong thuật ngữ của các toán hạng 8 bit. Khi thực hiện GOST bằng thiết bị, một vòng chính là việc thực hiện liên tiếp 3 phép toán của các tham số 32 bit : cộng, phép thế (được thực hiện đồng thời tại cả 8 nhóm 4 bit) và phép cộng từng bit theo modulo 2. Phép dịch vòng không là một

phép toán riêng biệt, vì được đảm bảo bằng chuyển mạch đơn giản của các dây dẫn. Như vậy, với thực hiện bằng thiết bị một vòng mã yêu cầu thực hiện 106 phép toán cơ sở và công việc này không thể song song hóa được.

Đặc điểm của thuật toán Rijndael

Bây giờ chúng ta xét đến các đặc điểm của việc thực hành thuật toán Rijndael. Đây là một thuật toán định hướng theo byte, có nghĩa là hoàn toàn có thể phát biểu theo thuật ngữ của các phép tính theo byte. Trong thuật toán sử dụng rộng rãi các phép toán đại số trên trường hữu hạn, trong đó phép nhân trong GF(2^8) là khó thể hiện nhất. Việc thực hiện trực tiếp các phép tính đó dẫn đến một thể hiện không hiệu quả của thuật toán. Tuy vậy cấu trúc byte của mã pháp mở ra các khả năng mở rộng lớn cho việc lập trình. Phép thế byte theo bảng cùng với phép nhân sau đó với hằng số trong trường GF(2^8) có thể biểu diễn như là một phép thế theo bảng. Trong biến đổi xuôi có 3 hằng số được sử dụng (01, 02, 03) và vì thế cần có bảng 3 như vậy, còn trong biến đổi ngược có 4 hằng số (OE, 0D, 0B, 09). Khi tổ chức khéo quá trình mã thì phép dịch byte theo từng dòng của ma trận dữ liệu có thể không cần thực hiện. Khi viết cho các máy 32 bit có thể cài đặt phép thế theo byte và phép nhân phần tử ma trận dữ liệu với cột của ma trận M như là một phép thay 8 bit bằng 32 bit. Như vậy, tất cả chương trình cho một vòng mã của phương án khối dữ liệu 128 bit sẽ dẫn đến 4 lệnh tải các phần tử khóa vào thanh ghi, 16 lệnh tải byte vào thanh ghi và lấy từ bộ nhớ ra giá trị đã được đánh chỉ số. Giá trị này được sử dụng trong phép tính theo byte. Đối với các bộ xử lý Intel Pentium không có đủ số thanh ghi còn cần thêm 4 lệnh tải nội dung các thanh ghi vào bộ nhớ, như vậy trên những bộ xử lý đã chỉ ra một vòng mã theo thuật toán Rijndael có thể thực hiện sau 40 lệnh hoặc sau 20 nhịp của bộ xử ký có phép tính đến khả năng thực hiện song song các lệnh bởi bộ xử lý. Cho 14 vòng mã của một chu trình mã sẽ cần 280 nhịp, cộng thêm một số nhịp thêm vào để cộng thêm khóa. Thêm vào một số nhịp cho phép giữ chậm bên trong bộ vi xử lý, chúng ta nhận được đánh giá 300 nhịp cho một chu trình mã. Trên bộ xử ký Pentium Pro- 200 về mặt lý thuyết cho phép đạt đến tốc độ

khoảng 0,67 triệu khối trong một giây hay khoảng 8,5 Mbyte/s (Mỗi khối có 128 bit). Đối với các phương án có số vòng ít hơn thì tốc độ tăng lên theo tỉ lệ.

Phép tối ưu chỉ ra trên đây, tuy vậy yêu cầu tiêu tốn một lượng xác định bộ nhớ. Cho mỗi cột của ma trận M xây dựng vecto thay thế của mình từ 1 byte sang từ có 4 byte. Hơn nữa, cho vòng cuối cùng trong đó không có phép nhân với ma trận M, cần có một vecto thay thế riêng cùng kích cỡ. Điều này yêu cầu sử dụng 5 x 2^8 x 4=5 Kb bộ nhớ để lưu trữ các nút thay thế mã và cũng một lượng như thế cho khi dịch, tất cả là 10 KB. Đối với các máy tính hiện đại trên sơ sở Intel Petium dưới sự điều khiển của hệ điều hành Windows 9x/NT/2000 thì không là một yêu cầu gì lớn cả.

Kiến trúc định hướng theo byte của thuật toán Rijndael hoàn toàn cho phép thể hiện hiệu quả của nó trên các bộ vi xử lý 8 bit, chỉ sử dụng các phép tải vào/ra thanh ghi, lấy các byte đã được đánh chỉ số trong bộ nhớ và phép cộng bit theo modulo 2. Đặc điểm đã chỉ ra cũng cho phép thực hành lập trình hiệu quả của thuật toán. Một vòng mã cần thực hiện 16 phép thế theo byte cộng thêm ‘’loại trừ hoặc’’ theo bit trên các khối 128 bit, chúng có thể thực hiện trong 3 giai đoạn. Tổng lại là 4 thao tác cho một vòng hoặc 57 thao tác cho một chu trình mã 14 vòng có tính đến một số thao tác thêm cho phép cộng khóa theo modulo 2 tức là vào khoảng 2 lần ít hơn GOST. Vì thuật toán Rijndael có độ dài khối 2 lần lớn hơn, nên điều này dẫn đến ưu thế gấp 4 lần về tốc độ với điều kiện thực hiện máy trên cơ sở cùng một công nghệ. Chú ý rằng đánh giá trên chỉ là thô.

Khi đánh giá các đặc trưng thực tế tốc bằng chương trình của hai thuật toán trên nền Intel Petium, với thuật toán Rijndael chúng ta xem xét phương án có 14 vòng. Cho mỗi thuật toán. Bằng ngôn ngữ C đã viết một hàm tương đương để mã một khối, trong đó có các dãy các vòng được trải ra ở dạng mã tuyến tính điều này cho phép đạt được tốc độ tối đa. Trong những hàm tương đương sử dụng các thông tin khóa ngẫu nhiên và các nút thay thế ngẫu nhiên, nhưng điều đó không ảnh hưởng gì đến tốc độ thi hành bởi vì tốc độ thực hiện của các lệnh

được sử dụng không phụ thuộc vào các toán hạng của nó. Các hàm thực hiện được việc mã được gọi hàng chục triệu lần và đo thời gian nó chạy, con số này được dùng làm chỉ số về tốc độ. Để biên dịch và xây dựng modulo thực thi đã sử dụng trình dịch Intel C++ v 4.5, vì nó cho phép nhận mã lệnh với tốc độ cao nhất. Cũng đã thử nghiệm với các trình biên dịch MS Visual C++ v 6.0, Boland C ++ v 5.5 và C++ v 2.95.2, nhưng mã nhận được khi sử dụng chúng cho tốc độ kém hơn. Mã được tối ưu hóa đối với các bộ xử lý Intel Petium và Intel Petium Pro/II/III. Với sự giúp đỡ của các bài toán thử nghiệm, tốc độ thực hiện các mã pháp đã được đo trên các bộ xử lý Intel Petium 166 MHz và Intel Petium III 433 MHz. Kết quả đo ở trong bảng sau :

Bộ xử lý	GOST 28147- 89	Rijndael 14 vòng
Petium 166	2,04 Mbyte/s	2,46 Mbyte/s
Petium III 433	8,03 Mbyte/s	9,36 Mbyte/s

Các chỉ số về tốc độ thực hiện của các thuật toán được so sánh

Như vậy, các thuật toán được xem xét có tốc độ so sánh được với nhau khi thực hiện trên nền 32 bit. Trên các nền 8 bit, bức tranh có lẽ cũng như vậy. Còn đối với việc cài đặt trên phần cứng khác với thuật toán mã GOST, Rijndael cho phép đạt được một mức độ song song hóa cao khi thực hiện thuật toán vì thao tác với các khối có kích thước nhỏ hơn và số vòng ít hơn, nên về mặt lý thuyết việc cài đặt cứng nó sẽ đạt được tốc độ nhanh hơn so với GOST trên cùng một nền công nghệ theo các đánh giá thô vào 4 lần.

Việc so sánh được tiến hành trên đây cho các tham số của 2 thuật toán mã hóa GOST 28147 – 89 và Rijndael đã chỉ ra rằng, mặc dù có sự khác biệt đáng kể trong nguyên tắc kiến thiết mà các mã pháp dựa vào, các thông số làm việc chính là gần như nhau. Điểm ngoại trừ là gần như chắc chắn Rijndael có ưu thế hơn về tốc độ so với GOST khi cài đặt máy trên cùng một công nghệ. Theo các tham số quan trọng về độ bền vững cho những thuật toán dạng đó, không thuật toán nào có được ưu thế đáng kể, ngay cả tốc độ của một chương trình tối ưu

trên bộ xử lý Intel Petium là cũng như nhau, điều này có thể ngoại suy ra mọi bộ xử lý 32 bit hiện đại khác.

Như vậy, có thể rút ra kết luận là chuẩn mã dữ liệu của nước Nga đáp ứng được các yêu cầu của các mã pháp hiện đại và có thể là chuẩn trong một thời gian dài nữa. Bước dễ thấy tiếp theo trong việc tối ưu hóa nó có thế là việc chuyển phép thế trong các nhóm 4 bit sang phép thế theo byte, điều này sẽ làm tăng hơn nữa tính bền vững của thuật toán với dạng phân tích mã đã biết.

3.8 So sánh chuẩn chữ ký số DSS với chuẩn chữ ký số GOST P34.10 - 2001

Nhìn chung hai chuẩn này cách thức tương tự nhau, song một số điểm khác nhau là

Tiêu chí	DSS	GOST P34.10-2001
Hàm băm	160 bit	256 bit
Tham số	P=512bit, q=160 bit	$2^{509}<p<2^{512}$,$2^{1020}<p<2^{1024}$ $2^{254}<q<2^{256}$
Hộp thay thế S-box	Cố định	Thay đổi theo tuần, tháng
Áp dụng	Toàn thế giới	Nước Nga
Ưu điểm	Linh động, tùy chọn	An toàn cao
Nhược điểm	Dễ dò tìm tấn công	Tốc độ chậm, lưu trữ lớn

Hàm băm

Chuẩn chữ ký số Nga, hàm băm có độ dài 256 bit lớn hơn của chuẩn chữ ký DSS 160 bit. Việc tăng độ dài giá trị hàm băm làm giảm xác xuất đụng chạm, tương ứng với nó là bậc của phần tử sinh, điều này làm cho việc giải bài toán logarithm rời rạc sẽ khó hơn khi cần tìm khóa bí mật.

Chọn tham số

Chuẩn chữ ký số của Nga được lập sau phương án chuẩn của nước Mỹ, cho nên các tham số của thuật toán này được chọn với trù tính về khả năng tiềm tàng

của người mã thám trong việc thám mã. Tăng độ dài phép cho phép modulo nguyên tố p, tức là một cách tương ứng tăng độ phức tạp của việc tính logarit rời rạc và làm khó hơn việc giả mạo chữ ký.

Hộp thay thế S- box

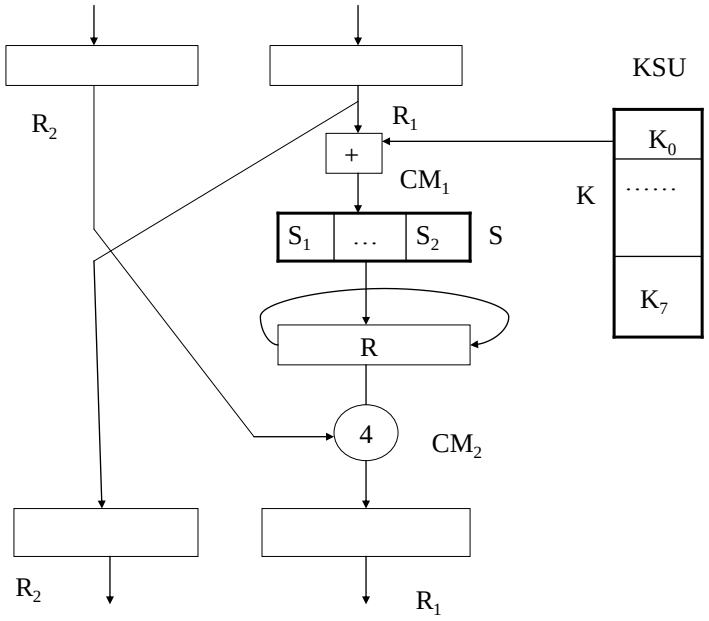
Chuẩn chữ ký số Nga GOST P34.10 – 2001 có hộp S- box thay đổi liên tục theo thời gian liên tục khác chữ ký sô DSS hộp thay đổi S-box cố định trong thời gian dài. Việc này làm cho chuẩn chữ ký số Nga trở lên an toàn cao hơn.

Chương 4 Nhận xét và kết luận về thuật toán mã hóa Liên Bang Nga

4.1 Mở đầu

Mô tả chi tiết của thuật toán mã hóa của Liên Bang Nga đã được công bố trong GOST 28147 - 89. Mục đích của những người thiết kế là cung cấp một thuật toán mã hóa có độ mật mềm dẻo. Thuật toán là một ví dụ của hệ mật kiểu DES cùng với lịch trình khóa được đơn giản hóa tối đa, nó mã bản thông báo 64 bit thành bản mã có 64 bit bằng khóa 256 bit.

4.2 Mô tả thuật toán GOST



Hình 1. Đường đi của dữ liệu trong một vòng mã/dịch của GOST

Thuật toán gồm 32 vòng lặp, (hai lần nhiều hơn DES). Mỗi vòng lặp được chỉ ra ở hình 1. Có 2 phần tử bí mật là khóa mật mã K 256 bit gồm 8 từ 32 bit lưu KSU, và hộp S-box S_1,....S_8.

Khóa mật mã K=($K_{0,.....,}$ K_7) được lưu trữ trong thiết bị lưu trữ khóa (KSU-key storage unit) như một dãy của 8 từ 32 bit ($K_{0,.....,}$ K_7). Mỗi từ khóa 32 bit K_i được gọi khóa thành phần (i=0,....,7). Để mã bản rõ 64 bit, trước hết nó được chia bản rõ ra làm 2 nửa 32 bit và được đặt vào thanh ghi R_1và R_2. Nội dung

của thanh ghi được cộng theo modulo 2^{32} vào khóa thành phần K_0 (bộ cộng CM_1), tức là: $R_1+K_0(\text{mod } 2^{32})$.

Dãy thu được chia 8 khối 4 bit. 8 khối 4 bit này là đầu vào của hộp S-box tương ứng S_1,..., S_8. Mỗi S_i là một hoán vị, 8 đầu ra khối 4 bit của hộp S-box được lưu trong thanh ghi dịch R, nội dung thanh ghi này dịch trái 11 bit cao(về phía bit bậc cao). Nội dung của thanh ghi R bây giờ được cộng modulo 2 với nội dung thanh ghi R_2 bằng bộ cộng CM_2. Nội dung từ sẽ được lưu trong R_1 và giá trị cũ được lưu trong R_2. Đến đây kết thúc vòng lặp thứ nhất.

Các vòng lặp khác tương tự như vòng thứ nhất. Trong vòng lặp thứ 2, chúng ta sử dụng khóa k_1 từ KSU. Các vòng lặp thứ 3, 4, 5, 6, 7, 8 sử dụng tương ứng các khóa thành phần k_2, k_3,....., k_7. Các vòng lặp thứ 9 đến 16 và từ 17 đến 24 cũng sử dụng các khóa thành phần này. Các vòng lặp 25 đến 32 sử dụng khóa thành phần theo thứ tự ngược lại, tức là vòng lặp thứ 25 sử dụng khóa k_7, vòng lặp thứ 26 sử dụng khóa k_6 và cứ tiếp tục như vậy. Vòng lặp cuối cùng dùng khóa k_0. Cho nên thứ tự của các khóa thành phần trong 32 vòng lặp là: k_0,....k_7, k_0,....k_7, k_0,....k_7, k_7,....k_0

Sau 32 vòng lặp, đầu ra từ bộ cộng CM_2 được đặt trong R_2, còn R_1 giữ nguyên giá trị cũ. Nội dung của các thanh ghi R_1 và R_2 là bản mã 64 bit cho bản rõ có 64 bit.

4.3 Các tính chất tổng quát của GOST

Thuật toán GOST lặp lại cấu trúc tổng thể của DES. Rõ ràng là những người thiết kế nó đã cố gắng để đạt được sự cân bằng giữa tính hiệu quả của thuật toán và độ mật của nó. Nó sử dụng các khối được xây dựng thường lệ và đơn giản. Đặc biệt, GOST khác DES ở những điểm sau:

1. Lịch trình khóa phức tạp được bỏ qua thay vào là dãy có quy tắc của các khóa thành phần

2. Khóa mật mã có độ dài 256 bit so với 56 bit của DES. Hơn nữa, lượng thực tế thông tin mật trong hệ thống, bao gồm cả các S-box gộp lại xấp xỉ 610 bit thông tin.

3. 8 hộp S- box S_1,.....S_8 là các hoàn vị $GF(2^4) \rightarrow GF(2^4)$, về tổng thể chỉ đòi hỏi không gian lưu trữ tương đương với 2 S- box của DES

4. khóa con cho mỗi vòng lặp là 32 bit cho phép cộng có nhớ chứ không phải là phép XOR 48 bit của DES

5. Phép hoán vị khối bất qui tắc P trong DES được thay bởi thanh ghi dịch đơn giản R, nó quay nội dung đi 11 bit về bên trái sau mỗi vòng.

6. Số vòng được tăng từ 16 lên 32.

Do độ mật của thuật toán phụ thuộc cả vào khóa mật mã và 8 phép thế S_i i=1,....,8, nên người sử dụng cần phải biết nên chọn 2 thành phần bí mật này như thế nào? Khóa mật mã có thể chọn ngẫu nhiên, nhưng việc chọn các hoán vị S_i được dành cho người có chức trách, người biết chọn những hoán vị tốt. Từ quan điểm của người sử dụng, độ mật được liên quan tới tính bảo mật của khóa K. Chú ý rằng người có trách nhiệm có thể chọn các S – box sao cho họ có thể phá được hệ mật (ví dụ, bằng cách chọn các hoán vị tuyến tính hay affine).

Chúng ta hãy xem xét cấu trúc của thuật toán GOST, bạn có thể hỏi xem phải chăng việc sử dụng các hoán vị thay cho một lớp lớn hơn nhiều tất cả các hàm số có thể làm giảm độ an toàn? Even và Goldreich đã chứng minh rằng một phép mã kiểu DES bất kỳ với một phép lặp.

$$L' = R$$

$$R' = L \oplus f(R,K)$$

Sinh ra một nhóm luân phiên với f: $GF(2^{32}) \rightarrow GF(2^{32})$ là hàm boolean, đầu vào là (L, R). Sau đó Pieprzyk và Zhang đã chỉ ra rằng nếu f là hoán vị thì hàm mã kiểu DES vẫn sinh ra nhóm luân phiên. Như vậy, việc sử dụng các hoán vị thay cho các hàm không làm suy giảm độ mật của thuật toán khi xem xét với một số vòng lớn.

Việc kết nối của CM_1, các S – box và phép dịch vòng R có thể xem như hàm vòng F. Hàm F ánh xạ chuỗi đầu vào 32 bit. Phần trung tâm của hàm F là 8 S – box kích thước 4*4. Trước hết, hàm F thực hiện việc chia chuỗi đầu vào 32 bit

thành 8 khối, mỗi khối 4 bit, và sau đó thay mỗi khối bằng 4 bit được định ra bởi S- box tương ứng.

Bạn có thể thấy các bit ra của hàm F bị ảnh hưởng bởi các tổ hợp khác nhau của đầu vào phụ thuộc vào vị trí của nó. Điều này được giải thích bởi tính chất của việc kết nối phép cộng modulo 2^{32} và các S- box. Phép cộng modulo 2^{32} tạo đầu ra là phi tuyến tất cả (trừ một trường hợp bit ra có nghĩa nhỏ nhất). Điều này dẫn chúng ta tới bổ đề.

Bổ đề 1: Các đầu ra của S_i bị ảnh hưởng bởi 4i bit của bản rõ từ thanh ghi R_1 và 4i bit của khóa thành phần (i=1, ...,8)

Vị trí của S_1 làm cho nó đặc biệt dễ bị tổn thương đối với tấn công tuyến tính. Hoán vị S_1 được chọn cẩn thận nhất sao cho đầu ra của S_1 có độ phi tuyến tối đa. Nếu quan tâm đến hàm F thì GOST hoàn toàn sánh được với DES vì nó có quan hệ giữa đầu vào /đầu ra phức tạp hơn.

Một vấn đề hết sức thú vị là việc chọn các S –box sao cho nó có tính phi tuyến cao. Nói chung, phép cộng làm tăng tính tuyến tính, nhưng cũng có trường hợp nó làm suy giảm độ phi tuyến của hàm F đến mức kém hơn độ phi tuyến của chính các S- box.

4.4 Các phép dịch vòng R trong GOST

Ảnh hưởng chính của hàm vòng là cung cấp tính khuyếch tán. Để nghiên cứu điều này, chúng ta giả sử rằng KSU = 0. Trước hết chúng ta chỉ tập trung vào hiệu ứng trộn của phép dịch vòng trong một nhánh của thuật toán Xét 2 trường hợp của thuật toán ở chế độ thay thế đơn giản.

1. Các S-box là ánh xạ đồng nhất
2. Các S- box là các hàm căng hoàn toàn có nghĩa là mỗi bit vào ảnh hưởng đến mọi đầu ra của S- box, hay tương đương là mỗi bit ra phụ thuộc vào mọi bit vào.

Ký hiệu R_l^i là đầu vào của nửa bên phải của thuật toán tại vòng thứ i và a_0^i,...a_{31}^i là từng bit đầu vào tại vòng này.

trường hợp 1: Các S-box là ánh xạ đồng nhất.

Xem xét các bit ảnh hưởng bởi a^1_0, bit đầu vào thứ nhất của vòng 1. Ta có:

$a^1_0 \rightarrow a^2_{11} \rightarrow a^3_{22} \rightarrow a^4_1 \rightarrow a^5_{12} \rightarrow a^6_{23} \rightarrow a^7_2 \Rightarrow$

$a^{10}_3 \Rightarrow a^{13}_4 \Rightarrow a^{16}_5 \Rightarrow a^{19}_6 \Rightarrow a^{22}_7 \Rightarrow a^{28}_9 \Rightarrow a^{31}_{10}$

Ký hiệu $\Rightarrow$ có nghĩa là sau 3 vòng lặp. Như vậy sau 32 vòng lặp thì a^1_0 ảnh hưởng tới tất cả các bit khác của một nửa R_1 đúng một lần. Dễ thấy mọi phép dịch vòng rot(j) khác (dịch R_1 đi i vị trí) cũng có tính chất này nếu như gcd(i,32)=1, hay i là lẻ.

Trường hợp 2: Các S-box là hàm căng hoàn toàn

Xét ảnh hưởng của bit a_0^1 trong trường hợp đầu vào của S-box ảnh hưởng tới mọi bit ra. Ảnh hưởng của bit này được lan truyền tới tất cả 32 bit của R_1 chỉ sau 8 vòng. Chúng ta chú ý rằng $a^1_0 \Rightarrow a^4_0 \rightarrow a^5_0 \Rightarrow a^7_0 \rightarrow a^8_0$

Trong đó → chỉ một vòng lặp còn => chỉ nhiều vòng lặp.

Mức độ lan truyền của mỗi vòng xác định các mối phụ thuộc hàm, có nghĩa là nếu tại vòng 1, 16 bit được ảnh hưởng thì một bit bị ảnh hưởng tại vòng 4 phụ thuộc vào 16 bit đầu vào.

Chúng ta chú ý rằng nếu phép dịch vòng là không phải bội 4 thì sự lan truyền xảy ra và 8 vòng là con số cần thiết để ảnh hưởng tới tất cả mọi bit của R_1. Tuy nhiên việc lan truyền phụ thuộc vào phép dịch. Ví dụ, nếu phép dịch là rot(1) thì ảnh hưởng của a^1_0 không đến được a^i_{31} với i<8. chúng ta có thể so sánh các phép quay vòng bằng cách đưa ra độ đo p(i) đó là số vòng nhỏ nhất cần thiết để các bit bị ảnh hưởng chiếm tất cả các vị trí trong R_1. Chúng ta đã thấy rằng p(1)=8 và p(11)=4.

Vì gcd(i, 32)=1 nên hoặc $i \equiv 1 (\mathrm{mod}\ 4)$. Bây giờ, thay đổi 1 hoặc 3 bit đầu vào ảnh hưởng tới cả 4 bit đầu ra của S -box. Cho nên để so sánh ảnh hưởng của các phép quay chúng ta chỉ cần xem xét các phép quay rot(i) với hoặc i=1, 5, …29 hoặc i= 3, 7, .. 31 p(i) hoàn toàn được xác định bằng thương của i chia cho 4. Từ chú ý này chúng ta kết luận rằng số vòng nhỏ nhất sao cho các bit bị ảnh hưởng bởi a^1_0 bao phủ tất cả các vị trí trong R_1 ít nhất một lần được ra như trong bảng 1. Chúng ta chú ý rằng giá trị nhỏ nhất p(i) bằng 4, điều này xảy ra với các

phép quay rot(9), rot (11), rot(21), rot(23). Có thể thấy rằng số vòng nhỏ nhất cần thiết cho khuyếch tán thành khối 8 bit sau 2 vòng. Sau 3 vòng, khối 8 bit khuyếch tán thành khối 12 bit. Mặc cho các khối này được sắp xếp như thế nào chúng vẫn không phủ hết 32 bit(Nhiều nhất nếu chúng không có vùng chung, chúng sẽ phủ 4+8+12=24 bit). Cho nên ít nhất cần 4 vòng để có khuyếch tán hoàn toàn.

Bảng 1. Sự lan truyền gây ra bởi phép quay

Rot(i)	1/3	5/7	9/1	13/1	17/1	21/2	25/2	29/3
P(i)	8	5	4	5	5	4	5	8

Cũng chú ý rằng 11 và 23 không là ước của 2^{32}-1, đó là modulos của bộ cộng CM_4 (bộ cộng CM_4 được sử dụng trong chế độ dòng.). Điều này có ảnh hưởng tới quyết định chọn phép quay 11 bit cho thanh ghi dịch vòng.

Trong phân tích trên chúng ta còn chưa tính đến việc đổi 2 nửa. Để nghiên cứu việc này chúng ta có thể bắt đầu thuật toán với R_2=0. Giả sử R_2^i ký hiệu đầu vào bên tay trái của thuật toán tại vòng thứ i, chúng ta cũng ký hiệu rot(i) bởi r_i và S là ánh xạ sinh bởi S-box. (S: $GF(2^{32})$→ $GF(2^{32})$). Cùng với các qui ước này, các phương trình tượng trưng cho 2 vòng của thuật toán là:

$R_1^2= R_1 \oplus r_iSr_iSR_i$, $R_2^2= r_iS_1R_1$

Và sau 3 vòng là

$R_1^3= r_iSR_1 \oplus r_iS(R_i \oplus r_iSr_iSR_1)$;

$R_2^3= R_1 \oplus r_iSr_iSR_1$.

Nếu ta giả thiết rằng $r_iS(R_i \oplus r_iSr_iSR_1)= r_iSR_i \oplus r_iSr_iSR_1$

Chúng ta có thể nói một điều gì đó về tính khuyếch tán của R_1 bởi hai nửa. Sử dụng quan hệ này, chúng ta thấy rằng sau 5 vòng cả R^5_1 và R^5_2 đều chứa thành phần $r_1Sr_iSr_iSR_1$. Nhưng cái này có thể viết lại nếu sử dụng dữ kiện là $r_iS=S'r_i$ với S' nào đó (các r_i và các S- Box tạo thành nhóm) cho nên:

$r_1Sr_iSr_iSR_1=S^{(4)}r_1{}^4R_1$. ($S^{(n)}$ ký hiệu tổ hợp của n S-box, tức là tích của các hoán vị được sinh ra). Theo bảng 1, chúng ta thấy rằng 5 vòng là yêu cầu cho tính khuyếch tán theo cả hai bên cho thuật toán với các phép quay rot(9), rot(11), rot(21), rot(23).

4.5 Lựa chọn các S-box

Chúng ta chú ý rằng GOST có độ dài khóa hữu ích xấp xỉ 610 bit, trong đó 256 bit được sử dụng để biểu diễn khóa còn các bít còn lại biểu diễn các S-box.

Hộp S-box có 8 hộp, là phép hoán vị của số nguyên [0,1,2...,15] và có cả thảy $16! \cong 2^{442}$ ánh xạ như vậy. Từ đó suy ra rằng cần $354 \cong 8*44.2$ bit để chỉ ra 8 S-box ngẫu nhiên từ tập tất cả các hoán vị 4 bit, tựu trung lại là 610=256+354 bit khóa. Để giảm độ dài của khóa, những người thiết kế có thể làm bằng cách sinh ra một tập các S-box có kích thước tương đối nhỏ, ví dụ 10000 và sử dụng khóa để chỉ ra S- box trong tập được chọn cố định ấy.

Như đã nói ở trên, tập tất cả các S-box là rất lớn, và không cho phép vét cạn để tìm ra S-box làm tối ưu hóa các tiêu chuẩn. Các thí nghiệm đã được làm bằng cách chọn ngẫu nhiên các S-box, sau đó các S-box được kiểm tra tính thích hợp bằng tấn công vi sai và tấn công tuyến tính.

Kết luận

Kết quả thu được qua nghiên cứu, tìm hiểu chuẩn chữ ký số Liên Bang Nga.

- Nắm lý thuyết mật mã học cơ sở lý thuyết nghiên cứu chữ ký số.
- Tìm hiểu một số chữ ký số tiêu biểu : RSA, Elgamal, DSS, hàm băm và ứng dụng.
- Tìm hiểu nghiên cứu chuẩn chữ ký số Liên Bang Nga đang sử dụng là chuẩn chữ ký số GOST P34.10 – 94 và GOST P34.10 – 2001.

Kết quả quan trọng nhất thu được qua đồ án này là thuật toán Gost về mặt cấu trúc tổng thể không khác DES là mấy song chuẩn chữ ký số Nga đã xây dựng dựa trên kinh nghiệm của thế giới, và khắc phục được các nhược điểm và những khả năng không thực hiện được của DES.

Chuẩn chữ ký số Nga năng suất và tiện lợi khi thể hiện như thế nào ?

- Thuận tiện thể hiện trong thiết bị cũng như phần mềm.
- Thể hiện hiệu quả chuẩn mã phần lớn trên máy tình hiện đại và các thẻ thông minh.
- Khả năng thực hiện hiệu quả trên các bộ vi xử lý 8 bit.
- đáp ứng được các yêu cầu của mã pháp hiện đại và có thể là chuẩn trong thời gian dài nữa.

Hướng phát triển

- Cài đặt ứng dụng cụ thể thực tiễn.
- Áp dụng thực tiễn vào công nghệ thông tin ở Việt Nam như vấn đề chính phủ điện tử ...

Các tài liệu tham khảo

[1]. **Phan Đình Diệu** (2000) Giáo trình an toàn thông tin và mật mã (ĐHQG HN)

[2]. **Nguyễn Ngọc Cương** 2003) Bài giảng An Toàn Thông Tin (DDHDL PĐ)

[3]. **Trịnh Nhật Tiến** (2008) Giáo trình An Toàn Thông Tin.

[4]. **Neal Koblitz** A Course in Number Theory and Cryptography

[5]. **AlfoedJ. Merezes** Hand book of Applied Cryptography, 2000

[6]. **С.Г.Барметв, В.В.Г.Таров, Р.Е.Серов** cơ sở của mật mã học hiện đại NXB Mockba, Tạp chí điện tử viễn thông năm 2002 trang (96 – 100)

[7]. **С.Г.Барметв, В.В.Г.Таров, Р.Е.Серов** cơ sở của mật mã học hiện đại NXB Mockba, Tạp chí điện tử viễn thông năm 2005.