Kỷ yếu Hội nghị KHCN Quốc gia lần thứ XI về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR); Hà Nội, ngày 09-10/8/2018
DOI: 10.15625/vap.2018.00042

MỘT PHƯƠNG PHÁP PHÁT TRIỂN HỆ MẬT KHÓA CÔNG KHAI

Nguyễn Lương Bình, Lưu Hồng Dũng, Tống Minh Đức
Khoa CNTT, Học viện Kỹ thuật Quân sự
nluongbinh@yahoo.co.uk, luuhongdung@gmail.com, ductm08@gmail.com

TÓM TẮT: *Bài báo đề xuất xây dựng hệ mật mã khóa công khai từ việc phát triển thuật toán ElGamal. Ngoài tính năng bảo mật thông tin, các thuật toán mới đề xuất còn có cơ chế xác thực tính toàn vẹn và nguồn gốc của bản tin được bảo mật, từ đó có thể chống lại các dạng tấn công giả mạo trong thực tế.*

Từ khóa: *Hệ mật khóa công khai, thuật toán mật mã khóa công khai, thuật toán mã hóa ElGamal, thuật toán chữ ký DSA.*

I. ĐẶT VẤN ĐỀ

Các thuật toán về hệ mật nói riêng và mật mã khóa công khai điển hình được sử dụng trong thực tế hiện nay như RSA [1] hay ElGamal [2] đều không có cơ chế xác thực nguồn gốc cũng như tính toàn vẹn của bản tin được mã hóa, nên không có khả năng chống lại các tấn công giả mạo như "*Man- in- the- Middle*" hay một số dạng tấn công khác [3]. Điều đó đã phần nào hạn chế khả năng ứng dụng của chúng trong thực tế. Trong [4-6] đã đề xuất phương pháp phát triển thuật toán mật mã khóa công khai có khả năng xác thực nguồn gốc và tính toàn vẹn của bản tin được mã hóa trên cơ sở tích hợp thuật toán mã hóa ElGamal với một thuật toán chữ ký số, các thuật toán này được gọi chung là SigCrypt và có thể chống lại các dạng tấn công giả mạo đã biết trong thực tế.

Trong bài báo này, nhóm tác giả tiếp tục đề xuất một phương pháp xây dựng hệ mật khóa công khai từ việc phát triển thuật toán ElGamal. Khác với các thuật toán SigCrypt trong [4-6], các thuật toán ở đây không xây dựng theo phương pháp tích hợp thuật toán ElGamal với thuật toán chữ ký số, song vẫn có khả năng xác thực nguồn gốc và tính toàn vẹn của các bản tin được bảo mật.

II. PHÁT TRIỂN HỆ MẬT KHÓA CÔNG KHAI ELGAMAL

2. 1. Thuật toán mật mã ElGamal và ElGamal - DSA SigCrypt

Mục này trình bày lại thuật toán mã hóa ElGamal và một thuật toán SigCrypt dựa trên việc tích hợp thuật toán ElGamal [2] và thuật toán chữ ký DSA [7], với mục đích làm cơ sở đánh giá về độ an toàn và hiệu quả thực hiện cho các thuật toán đề xuất ở mục sau.

Thuật toán mã hóa ElGamal

Giả thiết người gửi (mã hóa) ở đây là A, còn người nhận (giải mã) là B. Để gửi bản tin M cần bảo mật cho B, trước tiên A và B cùng thống nhất lựa chọn các tham số và hình thành khóa, rồi mã hóa và giải mã bản tin theo các thủ tục như sau:

a) Thủ tục hình thành khóa

Thủ tục được thực hiện bởi A và B, bao gồm các bước như sau:

[1]. Sinh số nguyên tố p lớn, mạnh sao cho việc giải bài toán logarit rời rạc trên Z_p là khó.

[2]. Chọn khóa bí mật: $1 < x < p$.

[3]. Tính khóa công khai: $y = g^x \bmod p$, ở đây: g là phần tử sinh của Z_p.

b) Thủ tục mã hóa

Thủ tục được thực hiện bởi người gửi A, bao gồm các bước như sau:

[1]. Biểu diễn bản tin cần mã hóa M thành một giá trị m tương ứng trong khoảng [0, p - 1]

[2]. Chọn ngẫu nhiên một giá trị k trong khoảng (1, q), rồi tính thành phần thứ nhất của bản mã:

$$C = m \times (y_B)^k \bmod p$$

[3]. Tính thành phần thứ hai của bản mã:

$$R = g^k \bmod p$$

[4]. Gửi bản mã (C,R) cho B.

c) Thủ tục giải mã:

Thủ tục được thực hiện bởi người nhận B, bao gồm các bước như sau:

[1]. Người nhận sử dụng khóa bí mật của mình để giải mã bản tin nhận được:

$$m = C \times (R)^{-x_B} \bmod p$$

[2]. Chuyển giá trị *m* thành bản tin M ban đầu.

Nhận xét:

Từ thuật toán giải mã cho thấy, việc giải mã hoàn toàn có thể thực hiện được mà không cần bất kỳ thông tin nào về người gửi/mã hóa. Nghĩa là, người nhận/giải mã không thể biết chắc chắn ai là người đã gửi bản tin mã hóa cho mình. Điều đó cho thấy thuật toán không có khả năng chống lại các kiểu tấn công giả mạo như "*Man- in- the- Middle*" hay một số dạng khác [3].

Thuật toán ElGamal - DSA SigCrypt

Thuật toán ElGamal - DSA SigCrypt ở đây là một ví dụ minh họa cho việc tích hợp thuật toán mã hóa ElGamal với một thuật toán chữ ký số nhằm bảo đảm khả năng bảo mật và xác thực (nguồn gốc và tính toàn vẹn) thông tin một cách đồng thời, từ đó có thể chống lại các kiểu tấn công giả mạo trong thực tế. Thuật toán chữ ký số được sử dụng ở đây là DSA [7]. Cũng có thể tích hợp thuật toán ElGamal với một thuật toán chữ ký số khác như GOST R34.10 - 94 [8], Schnorr [9] bằng phương pháp tương tự [4-6].

Thuật toán ElGamal - DSA SigCrypt bao gồm các thủ tục hình thành tham số và khóa, thủ tục mã hóa và thủ tục giải mã như sau:

a) Thủ tục hình thành tham số hệ thống và khóa

[1]. Sinh 2 số nguyên tố lớn và mạnh: *p* và *q*, thỏa mãn: $q \mid (p-1)$.

[2]. Tính: $g = \alpha^{(p-1)/q} \bmod p$ với $\alpha \in Z_p^*$.

[3]. Chọn khóa bí mật *x* là một số nguyên thỏa mãn: $1 < x < q$.

[4]. Khóa công khai được tính theo công thức:

$$y = g^x \bmod p \tag{2.1.1}$$

[5]. Lựa chọn hàm băm: $H : \{0,1\}^* \mapsto Z_n$ với: $q < n < p$

[6]. Công khai các giá trị: *p, q, g, y.* Giữ bí mật: *x*.

b) Thủ tục mã hóa

Dữ liệu đầu vào bao gồm bản tin cần mã hóa M, khóa bí mật x_A của người gửi/mã hóa và khóa công khai y_A của người nhận/giải mã. Thủ tục bao gồm các bước như sau:

[1]. Biểu diễn bản tin cần mã hóa M thành một giá trị *m* tương ứng trong khoảng [0, p - 1].

[2]. Chọn ngẫu nhiên một giá trị *k* trong khoảng (1, q) và tính thành phần thứ nhất của bản mã:

$$C = m \times (y_B)^k \bmod p \tag{2.1.2}$$

[3]. Tính thành phần thứ 2 của bản mã:

$$R = g^k \bmod p \tag{2.1.3}$$

[4]. Tính thành phần thứ 3 của bản mã:

$$S = k^{-1} \times (H(M) + x_A \times R) \bmod q \tag{2.1.4}$$

[5]. Gửi bản mã (C, R, S) cho B.

Nhận xét:

Trong thuật toán này, thành phần R có chức năng kép. Đối với thuật toán mã hóa ElGamal, cặp (C,R) là bản mã của M. Đồng thời, cặp (R,S) ở đây cũng là chữ ký của người gửi/mã hóa do DSA tạo ra từ bản tin M. Điểm khác là trong DSA, thành phần R được tính theo (2.1.5):

$$R = (g^k \bmod p) \bmod q \tag{2.1.5}$$

Trong ElGamal - DSA SigCrypt, thành phần R cũng có thể được tính theo (2.1.5) để rút ngắn độ dài chữ ký, khi đó thành phần S cần phải được tính theo (2.1.6):

$$S = k^{-1} \times (H(C) + x_A \times R) \bmod q \tag{2.1.6}$$

Trường hợp này, cặp (R,S) là chữ ký tương ứng với C thay vì với M. Tuy nhiên, vai trò của (R, S) trong việc xác thực nguồn gốc và tính toàn vẹn của bản tin M là không thay đổi.

c) Thủ tục giải mã

Dữ liệu đầu vào bao gồm bản mã (C, R, S) và khóa công khai y_A của người gửi/mã hóa và khóa bí mật x_B của người nhận/giải mã. Thủ tục bao gồm các bước như sau:

[1]. Tính giá trị:

$$m = C \times (R)^{-x_B} \bmod p \tag{2.1.7}$$

[2]. Tính giá trị W:

$$W = S^{-1} \bmod q \tag{2.1.8}$$

[3]. Chuyển giá trị *m* thành bản tin *M* ban đầu và tính giá trị U:

$$U = W \times H(M) \bmod q \tag{2.1.9}$$

[4]. Tính giá trị V:

$$V = W \times R \bmod q \tag{2.1.10}$$

[5]. Tính giá trị $\overline{R}$:

$$\overline{R} = g^U \times (y_A)^V \bmod p \tag{2.1.11}$$

[6]. Kiểm tra nếu: $\overline{R} = R$ thì bản tin M được công nhận về nguồn gốc và tính toàn vẹn.

Chú ý:

Khi các thành phần (R, S) được tính theo (2.1.5) và (2.1.6) thì thứ tự các bước thực hiện của *Thủ tục giải mã* cũng cần thay đổi lại như sau:

[1]. Tính giá trị W:

$$W = S^{-1} \bmod q$$

[2]. Tính giá trị U:

$$U = W \times H(C) \bmod q$$

[3]. Tính giá trị V:

$$V = W \times R \bmod q$$

[4]. Tính giá trị $\overline{R}$:

$$\overline{R} = g^U \times (y_A)^V \bmod p$$

[5]. Kiểm tra nếu: $\overline{R} \bmod q = R$ thì thực hiện bước [6] để giải mã bản tin. Ngược lại, nếu:

$\overline{R} \bmod q \neq R$ thì kết thúc thủ tục giải mã.

[6]. Giải mã bản tin nhận được:

$$m = C \times (\overline{R})^{-x_B} \bmod p$$

[7]. Chuyển giá trị *m* thành bản tin M ban đầu.

Nhận xét:

Trong trường hợp này, việc xác thực nguồn gốc và tính toàn vẹn của bản tin M sẽ được thực hiện gián tiếp qua bản mã C. Chỉ sau khi nguồn gốc và tính toàn vẹn của C được khẳng định thì việc giải mã bản tin mới được thực hiện.

d) Tính đúng đắn của thuật toán ElGamal - DSA SigCrypt

Điều cần chứng minh ở đây là: cho *p*, *q* là 2 số nguyên tố thỏa mãn điều kiện $q \mid (p-1)$, $g = \alpha^{(p-1)/q} \bmod p$ với: $1 < \alpha < p$, $H : \{0,1\}^* \mapsto Z_n$ với: $q < n < p$, $1 < x_A, x_B, k < q$, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$, $0 \le M \le p-1$, $C = M \times (y_B)^k \bmod p$, $R = g^k \bmod p$, $S = k^{-1} \times (H(M) + x_A.R) \bmod q$. Nếu: $\overline{M} = C \times (R)^{-x_B} \bmod p$, $W = S^{-1} \bmod q$, $U = W \times H(\overline{M}) \bmod q$, $V = W \times R \bmod q$ và: $\overline{R} = g^U \times (y_A)^V \bmod p$ thì: $\overline{R} = R$.

Thật vậy, từ (2.1.1), (2.1.2), (2.1.3) và (2.1.7) ta có**:**

$$\overline{M} = C \times (R)^{-x_B} \bmod p = \left(M \times (y_B)^k \bmod p\right) \times \left(g^k \bmod p\right)^{-x_B} \bmod p$$
$$= M \times g^{k.x_B} \times g^{-k.x_B} \bmod p = M \quad (2.1.12)$$

Từ (2.1.4), (2.1.8), (2.1.9), (2.1.10), (2.1.11) và (2.1.12) ta có:

$$\overline{R} = g^U \times (y_A)^V \bmod p = g^{W.H(\overline{M})} \times \left(g^{x_A} \bmod p\right)^{W.R} \bmod p$$
$$= g^{S^{-1}.H(M)} \times g^{x_A.S^{-1}.R} \bmod p = g^{S^{-1}.(H(M)+x_A.R)} \bmod p = g^k \bmod p \quad (2.1.13)$$

Từ (2.1.13) và (2.1.3), suy ra điều cần chứng minh: $\overline{R} = R$

Tính đúng đắn của ElGamal - DSA SigCrypt trong trường hợp (R, S) được tính theo (2.1.5) và (2.1.6) được chỉ ra trong [6].

e) Mức độ an toàn của thuật toán ElGamal - DSA SigCrypt

Để bảo đảm an toàn, các tham số {*p, q, g*} cần phải được lựa chọn tương tự như DSA [7] hay GOST R34.10-94 [8], với: $| p | \geq 512bit$, $| q | \geq 160bit$. Ngoài ra, giá trị *k* cũng không được phép sử dụng lặp lại khi mã hóa các bản tin khác nhau. Với các điều kiện như vậy, mức độ an toàn của thuật toán ElGamal - DSA SigCrypt đúng bằng mức độ an toàn của thuật toán mã hóa ElGamal về khía cạnh bảo mật và bằng với mức độ an toàn của thuật toán ký số DSA xét về khía cạnh chống giả mạo bản tin.

2.2. Một số thuật toán mật mã khóa công khai được phát triển từ thuật toán ElGamal

Mục này đề xuất xây dựng 2 thuật toán mật mã khóa công khai phát triển từ thuật toán ElGamal. Như đã đề cập ở trên, điểm khác biệt với các thuật toán Sigcrypt nói chung và thuật toán ElGamal - DSA SigCrypt nói riêng là các thuật toán đề xuất ở đây không xây dựng theo phương pháp tích hợp với thuật toán chữ ký số song vẫn có khả năng xác thực nguồn gốc và tính toàn vẹn của bản tin nhận được sau giải mã.

Thuật toán MTA 17.5 - 01

Thuật toán thứ nhất - ký hiệu MTA 17.5 - 01, được đề xuất ở đây bao gồm thủ tục hình thành tham số hệ thống và khóa tương tự như thuật toán ElGamal - DSA SigCrypt, trong đó cũng giả thiết người gửi/mã hóa là A có khóa bí mật và công khai tương ứng là x_A và y_A, người nhận/giải mã là B có cặp khóa bí mật và công khai tương tự là x_B và y_B, với:

$$y_A = g^{x_A} \bmod p \,,\; y_B = g^{x_B} \bmod p \quad (2.2.1)$$

Thuật toán bao gồm các thủ tục mã hóa và giải mã như sau:

a) Thủ tục mã hóa

Được thực hiện bởi A, bao gồm các bước như sau:

[1]. Biểu diễn bản tin cần mã hóa M thành một giá trị *m* tương ứng trong khoảng [0, p - 1], chọn ngẫu nhiên một giá trị *k* trong khoảng (1, q) rồi tính thành phần thứ nhất của bản mã:

$$C = m \times (y_B)^k \bmod p \quad (2.2.2)$$

[2]. Tính thành phần thứ 2 của bản mã:

$$R = g^k \bmod p \quad (2.2.3)$$

[3]. Tính giá trị:

$$S_A = (y_B)^{x_A} \bmod p \quad (2.2.4)$$

[4]. Tính thành phần thứ 3 của bản mã:

$$E = H(M \,||\, S_A) \bmod q \quad (2.2.5)$$

[5]. Gửi bản mã (C, R, E) cho B.

b) Thủ tục giải mã

Được thực hiện bởi B, bao gồm các bước như sau:

[1]. Người nhận sử dụng khóa bí mật của mình để giải mã bản tin nhận được:

$$\overline{m} = C \times (R)^{-x_B} \bmod p \quad (2.2.6)$$

[2]. Tính giá trị:

$$S_B = (y_A)^{x_B} \bmod p \tag{2.2.7}$$

[3]. Chuyển giá trị $\overline{m}$ thành bản tin $\overline{M}$, rồi tính giá trị:

$$\overline{E} = H(\overline{M} \,||\, S_B) \bmod q \tag{2.2.8}$$

[4]. Kiểm tra nếu: $\overline{E} = E$ thì $\overline{M} = M$ và người gửi được khẳng định là A.

c) Tính đúng đắn của MTA 17.5 - 01

Điều cần chứng minh ở đây là: Cho: p, q là 2 số nguyên tố thỏa mãn: $q \,|\, (p-1)$, $1 < \alpha < p$, $g = \alpha^{(p-1)/q} \bmod p$, $H : \{0,1\}^* \mapsto Z_n$ với: $q < n < p$, $1 < x_A, x_B < q$, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$, $1 < k < q$, $0 \le M \le p-1$, $C = M \times (y_B)^k \bmod p$, $R = g^k \bmod p$, $S_A = (y_B)^{x_A} \bmod p$, $E = H(M \,||\, S_A) \bmod q$. Nếu: $\overline{M} = C \times (R)^{-x_B} \bmod p$, $S_B = (y_A)^{x_B} \bmod p$, $\overline{E} = H(\overline{M} \,||\, S_B) \bmod q$ thì: $\overline{E} = E$.

Chứng minh:

Thật vậy, từ (2.2.1), (2.2.2) và (2.2.3) ta có:

$$\begin{aligned} \overline{M} &= C \times (R)^{-x_B} \bmod p = \left(M \times (y_B)^k \bmod p\right) \times \left(g^k \bmod p\right)^{-x_B} \bmod p \\ &= M \times g^{k.x_B} \times g^{-k.x_B} \bmod p = M \end{aligned} \tag{2.2.9}$$

Từ (2.2.1) và (2.2.4), ta có:

$$S_A = (y_B)^{x_A} \bmod p = \left(g^{x_B} \bmod p\right)^{x_A} \bmod p = g^{x_A.x_B} \bmod p \tag{2.2.10}$$

Mặt khác, từ (2.2.1) và (2.2.7):

$$S_B = (y_A)^{x_B} \bmod p = \left(g^{x_A} \bmod p\right)^{x_B} \bmod p = g^{x_A.x_B} \bmod p \tag{2.2.11}$$

Từ (2.2.10) và (2.2.11) suy ra: $S_A = S_B$ (2.2.12)

Thay (2.2.9) và (2.2.12) vào (2.2.8) ta được:

$$\overline{E} = H\left(\overline{M} \,||\, S_B\right) \bmod q = H(M \,||\, S_A) \bmod q \tag{2.2.13}$$

Từ (2.2.5) và (2.2.13) suy ra điều cần chứng minh: $\overline{E} = E$.

d) Mức độ an toàn của MTA 17.5 - 01

Thủ tục mã hóa và giải mã của MTA 17.5 - 01 thực chất cũng chính là thủ tục mã hóa và giải mã của thuật toán ElGamal. Vì thế, độ an toàn về khả năng bảo mật thông tin được mã hóa của MTA 17.5 - 01 sẽ bằng đúng độ an toàn của thuật toán mã hóa ElGamal.

Từ (2.2.5) của *Thủ tục mã hóa* và (2.2.8) của *Thủ tục giải mã* cho thấy điều kiện: $\overline{E} = E$ chỉ có thể được thỏa mãn khi đồng thời: $\overline{M} = M$ và: $S_B = S_A$. Nghĩa là, bản tin phải được bảo đảm về tính toàn vẹn và người gửi phải là A - đối tượng sở hữu x_A và y_A. Bằng việc sử dụng hàm băm an toàn (ví dụ: SHA - 256/512,…) ở (2.2.5) và (2.2.8), thì việc tạo được: $\overline{M} \neq M$ hay: $S_A \neq (y_B)^{x_A} \bmod p$, hoặc đồng thời cả hai ($\overline{M} \neq M$ và: $S_A \neq (y_B)^{x_A} \bmod p$) mà vẫn thỏa mãn: $\overline{E} = E$ là không khả thi. Như vậy, độ an toàn về khả năng chống tấn công giả mạo của MTA 17.5 - 01 có thể đánh giá bằng độ an toàn của hàm băm H(.) được sử dụng trong thuật toán.

e) Hiệu quả thực hiện của MTA 17.5 - 01

Hiệu quả thực hiện của thuật toán MTA 17.5 - 01 được đánh giá dựa trên việc so sánh với thuật toán ElGamal - DSA SigCrypt được chỉ ra trên các bảng 1 và bảng 2 như sau:

Bảng 1. Thuật toán mã hóa ElGamal - DSA SigCrypt và MTA 17.5 - 01

	ElGamal - DSA SigCrypt	**MTA 17.5 - 01**
Số phép tính lũy thừa	2	3
Số phép tính nhân	3	1
Số phép tính nghịch đảo	1	0
Số phép băm	1	1
Sinh số ngẫu nhiên	1	1
Kích thước bản mã	2|p| + |q|	2|p| + |q|

Bảng 2. Thuật toán giải mã ElGamal - DSA SigCrypt và MTA 17.5 - 01

	ElGamal - DSA SigCrypt	**MTA 17.5 - 01**
Số phép tính lũy thừa	3	2
Số phép tính nhân	4	1
Số phép tính nghịch đảo	2	1
Số phép băm	1	1

Thuật toán MTA 17.5 - 02

Thuật toán thứ hai - ký hiệu MTA 17.5 - 02, cũng giả thiết có thủ tục hình thành tham số hệ thống và khóa tương tự như như thuật toán ElGamal - DSA SigCrypt. Người gửi/mã hóa và người nhận/giải mã có các cặp khóa bí mật, công khai (xA, yA) và (xB, yB) như sau:

$$y_A = g^{x_A} \bmod p,\ y_B = g^{x_B} \bmod p \tag{2.3.1}$$

Thuật toán bao gồm các thủ tục mã hóa và giải mã như sau:

a) Thủ tục mã hóa

Được thực hiện bởi A, bao gồm các bước sau:

[1]. Tính giá trị:

$$S_A = (y_B)^{x_A} \bmod p \tag{2.3.2}$$

[2]. Tính giá trị:

$$k_A = H(M \,||\, S_A) \bmod q \tag{2.3.3}$$

[3]. Biểu diễn bản tin cần mã hóa M thành một giá trị *m* tương ứng trong khoảng [0, p - 1], rồi tính thành phần thứ nhất của bản mã:

$$C = m \times (y_B)^{k_A} \bmod p \tag{2.3.4}$$

[4]. Tính thành phần thứ 2 của bản mã:

$$R = g^{k_A} \bmod p \tag{2.3.5}$$

[5]. Gửi bản mã (C,R) cho B.

b) Thủ tục giải mã

Được thực hiện bởi B, bao gồm các bước như sau:

[1]. Người nhận sử dụng khóa bí mật của mình để giải mã bản tin nhận được:

$$\overline{m} = C \times (R)^{-x_B} \bmod p \tag{2.3.6}$$

[2]. Tính giá trị:

$$S_B = (y_A)^{x_B} \bmod p \tag{2.3.7}$$

[3]. Chuyển giá trị $\overline{m}$ thành bản tin $\overline{M}$, rồi tính giá trị:

$$k_B = H(\overline{M} \,||\, S_B) \bmod q \tag{2.3.8}$$

[4]. Tính giá trị:

$$\overline{R} = g^{k_B} \bmod p \tag{2.3.9}$$

[5]. Kiểm tra nếu: $\overline{R} = R$ thì $\overline{M} = M$ và người gửi được khẳng định là A.

c) Tính đúng đắn của MTA 17.5 - 02

Điều cần chứng minh ở đây là: Cho: p, q là 2 số nguyên tố thỏa mãn: $q \,|\, (p-1)$, $1 < \alpha < p$, $g = \alpha^{(p-1)/q} \bmod p$, $H : \{0,1\}^* \mapsto Z_n$ với: $q < n < p$, $1 < x_A, x_B < q$, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$, $0 \le M \le p-1$, $S_A = (y_B)^{x_A} \bmod p$, $k_A = H(M \,||\, S_A) \bmod q$, $C = M \times (y_B)^{k_A} \bmod p$, $R = g^{k_A} \bmod p$. Nếu: $\overline{M} = C \times (R)^{-x_B} \bmod p$, $S_B = (y_A)^{x_B} \bmod p$, $k_B = H(\overline{M} \,||\, S_B) \bmod q$ và: $\overline{R} = g^{k_B} \bmod p$ thì: $\overline{R} = R$.

Chứng minh:

Thật vậy, từ (2.3.1), (2.3.4), (2.3.5) và (2.3.6) ta có:

$$\overline{M} = C \times (R)^{-x_B} \bmod p = \left(M \times (y_B)^{k_A} \bmod p\right) \times \left(g^{k_A} \bmod p\right)^{-x_B} \bmod p \quad (2.3.10)$$
$$= M \times g^{k_A \cdot x_B} \times g^{-k_A \cdot x_B} \bmod p = M$$

Từ (2.3.1) và (2.3.2), ta có:

$$S_A = (y_B)^{x_A} \bmod p = \left(g^{x_B} \bmod p\right)^{x_A} \bmod p = g^{x_A \cdot x_B} \bmod p \quad (2.3.11)$$

Mặt khác, từ (2.3.1) và (2.3.7):

$$S_B = (y_A)^{x_B} \bmod p = \left(g^{x_A} \bmod p\right)^{x_B} \bmod p = g^{x_A \cdot x_B} \bmod p \quad (2.3.12)$$

Từ (2.3.11) và (2.3.12) suy ra: $S_A = S_B$ (2.3.13)

Thay (2.3.10) và (2.3.13) vào (2.3.8) ta được:

$$k_B = H\left(\overline{M} \,||\, S_B\right) \bmod q = H(M \,||\, S_A) \bmod q \quad (2.3.14)$$

Từ (2.3.3) và (2.3.14) suy ra: $k_B = k_A$ (2.3.15)

Thay (2.3.15) vào (2.3.9) ta có:

$$\overline{R} = g^{k_B} \bmod p = g^{k_A} \bmod p \quad (2.3.16)$$

Từ (2.3.5) và (2.3.16), suy ra điều cần chứng minh: $\overline{R} = R$.

d) Mức độ an toàn của MTA 17.5 - 02

Phân tích tương tự MTA 17.5 - 01 cho thấy, độ an toàn về khả năng bảo mật thông tin được mã hóa của thuật toán MTA 17.5 - 02 ở đây cũng đúng bằng độ an toàn của thuật toán ElGamal, còn độ an toàn về khả năng chống tấn công giả mạo của nó cũng được đánh giá bằng độ an toàn của hàm băm sử dụng trong thuật toán.

e) Hiệu quả thực hiện của MTA 17.5 - 02

Hiệu quả thực hiện của thuật toán MTA 17.5 - 02 được đánh giá dựa trên việc so sánh với thuật toán ElGamal - DSA SigCrypt được chỉ ra trên các bảng 3 và bảng 4 như sau:

Bảng 3. Thuật toán mã hóa ElGamal - DSA SigCrypt và MTA 17.5 - 02

	ElGamal - DSA SigCrypt	**MTA 17.5 - 02**
Số phép tính lũy thừa	2	3
Số phép tính nhân	3	1
Số phép tính nghịch đảo	1	0
Số phép băm	1	1
Sinh số ngẫu nhiên	1	0
Kích thước bản mã	2|p| + |q|	2|p|

Bảng 4. Thuật toán giải mã ElGamal - DSA SigCrypt và MTA 17.5 - 02

	ElGamal - DSA SigCrypt	**MTA 17.5 - 02**
Số phép tính lũy thừa	3	3
Số phép tính nhân	4	1
Số phép tính nghịch đảo	2	1
Số phép băm	1	1

III. KẾT LUẬN

Bài báo đề xuất phương pháp xây dựng hệ mật mật khóa công khai từ việc phát triển thuật toán mã hóa ElGamal. Các thuật toán xây dựng theo phương pháp đề xuất ở đây có tính năng bảo mật như thuật toán ElGamal, hơn nữa chúng còn có cơ chế xác thực nguồn gốc và tính toàn vẹn của bản tin được mã hóa, vì thế có thể chống lại hiệu quả các dạng tấn công giả mạo đã được biết trong thực tế.

IV. TÀI LIỆU THAM KHẢO

[1] R. L. Rivest, A. Shamir, and L. M. Adleman. “A Method for Obtaining Digital Signatures and Public Key Cryptosystems”. Commun. of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.

[2] T. ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". IEEE Transactions on Information Theory. 1985, Vol. IT-31, No. 4. pp.469-472.

[3] Mark Stamp, Richard M. Low. "Applicd cryptanalysis: Breaking Ciphers in the Real World". John Wiley & Sons, Inc., ISBN 978-0-470-1.

[4] Lưu Hồng Dũng, Trần Trung Dũng và Tống Minh Đức. "Nghiên cứu xây dựng hệ tích hợp mật mã khóa công khai - chữ ký số". Tạp chí Khoa học và Kỹ thuật (Học viện KTQS), số 149 (08-2012). ISSN: 1859 - 0209., 01/08/2012 .

[5] Lưu Hồng Dũng. "Phát triển thuật toán mật mã khóa công khai dựa trên hệ mật El Gamal". Chuyên san Các công trình nghiên cứu, phát triển và ứng dụng CNTT và TT, Bộ TT và TT, tập V-1, số 8(28) (12-2012). ISSN: 1859 - 3526., pp. 8, 01/12/2012.

[6] Lưu Hồng Dũng, Ngô Đăng Tiến, Trần Trung Dũng and Vũ Tất Thắng. "Phát triển một số thuật toán mật mã khóa công khai". Hội thảo quốc gia lần thứ XV: Một số vấn đề chọn lọc của Công nghệ Thông tin và Truyền thông. Hà Nội 3-4/12/2012. ISBN: 978 - 604 - 67 - 0645 - 8., pp. 6, 04/12/2012 .

[7] National Institute of Standards and Technology, NIST FIPS PUB 186-3. Digital Signature Standard, U.S. Department of Commerce, 1994.

[8] GOST R 34.10-94. Russian Federation Standard. Information Technology. Cryptographic data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm. Government Committee of the Russia for Standards, 1994 (in Russian).

[9] C. P. Schnorr. "Efficient signature generation by smart cards". Journal of Cryptology, vol. 4, pp. 161 - 174, 1991.

THE METHOD OF DEVELOPING PUBLIC-KEY ENCRYPTION ALGORITHMS

Nguyen Luong Binh, Luu Hong Dung,Tong Minh Duc

ABSTRACT: *In the cryptography branch, the Secure and authenticated message is one of the most important modern cryptography. To encrypt and authenticate we can be to signscription.To secure in the public key we can be which form the basis of the methods including RSA, ElGamal, and DSS. In this paper, we propose to create a public key cryptographic algorithm from the development of the ElGamal algorithm can be encrypted and authenticated [8] without signscription in many cases reduce the cost of registration and digital signature storage.*

Keywords: *cryptographic, algorithm cryptographic, algorithm ciphers ElGamal, algorithm signcription DSA.*