Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ IX "Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR'9)"; Cần Thơ, ngày 4-5/8/2016
DOI: 10.15625/vap.2016.00072

PHÁT TRIỂN THUẬT TOÁN MẬT MÃ KHÓA CÔNG KHAI DỰA TRÊN BÀI TOÁN LOGARIT RỜI RẠC

Lưu Hồng Dũng[1], Nguyễn Đức Thụy [2], Nguyễn Lương Bình [3], Tống Minh Đức [4]

[1] Khoa CNTT, Học viện Kỹ thuật Quân sự
[2] Khoa CNTT, Cao đẳng Kinh tế - Kỹ thuật Tp. Hồ Chí Minh
[3] Khoa CNTT, Học viện Kỹ thuật Quân sự
[4] Khoa CNTT, Học viện Kỹ thuật Quân sự

luuhongdung@gmail.com, thuyphulam2013@gmail.com, nluongbinh@yahoo.co.uk, ductm08@gmail.com

TÓM TẮT— *Bài báo đề xuất xây dựng thuật toán mật mã khóa công khai dựa trên tính khó của bài toán logarit rời rạc trên trường hữu hạn. Ngoài khả năng bảo mật thông tin, thuật toán mới đề xuất còn có thể 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 đã biết trong thực tế. Ngoài ra, thuật toán còn được thiết kế để hỗ trợ khả năng tương tác giữa các đối tượng tham gia trao đổi thông tin mật phù hợp với các yêu cầu đặt ra trong các ứng dụng thực tế.*

Từ khóa— *Mật mã khóa công khai, thuật toán mật mã khóa công khai, thuật toán chữ ký số, bài toán logarit rời rạc.*

I. ĐẶT VẤN ĐỀ

Các thuật toán mật mã khóa công khai điển hình được sử dụng trong thực tế hiên nay như RSA[1] hay ElGamal [2] đều không có cơ chế xác thực nguồn gốc cũng như tính toàn vẹn của bản tin nhận được nên không có khả năng chống lại các tấn công giả mạo trong thực tế kiểu như tấn công "*Man- in- the- Middle*" [3]. Ngoài ra, các thuật toán kiểu này cũng không hỗ trợ khả năng tương tác giữa các bên tham gia trao đổi thông tin mà các ứng dụng trong thực tế thường yêu cầu.

Trong bài báo này, nhóm tác giả đề xuất xây dựng thuật toán mật mã khóa công khai được tích hợp chữ ký số cho phép khả năng bảo mật và xác thực thông tin một cách đồng thời, có thể chống lại các dạng tấn công giả mạo một cách hiệu quả. Hơn nữa, thuật toán mới đề xuất còn được thiết kế dưới dạng một giao thức cho khả năng tương tác giữa các bên tham gia trao đổi thông tin nhằm phù hợp với yêu cầu của các ứng dụng trong thực tế. Đây là những vấn đề mà trên thực tế chưa có các kết quả nghiên cứu tương ứng được công bố.

II. PHÁT TRIỂN THUẬT TOÁN MẬT MÃ KHÓA CÔNG KHAI

A. Xây dựng thuật toán cơ sở

Thuật toán cơ sở ở đây là một thuật toán chữ ký số được xây dựng dựa trên tính khó của bài toán logarit rời rạc trên trường hữu hạn theo phương pháp chỉ ra trong [4] và được sử dụng để xây dựng các thuật toán mật mã khóa công khai có khả năng bảo mật và xác thực thông tin ở phần sau.

1. Bài toán logarit rời rạc

Bài toán logarit rời rạc – DLP (Discrete Logarithm Problem) có thể được phát biểu như sau: Cho p là số nguyên tố, g là phần tử sinh của nhóm $\mathbb{Z}_p^*$. Với mỗi số nguyên dương $y \in \mathbb{Z}_p^*$, hãy tìm x thỏa mãn phương trình:

$$g^x \bmod p = y$$

Ở đây, bài toán logarit rời rạc được sử dụng với vai trò hàm một chiều trong việc hình thành khóa của các thực thể trong cùng hệ thống với bộ tham số $\{p,g\}$ dùng chung. Dễ thấy rằng, nếu x là khóa bí mật thì việc tính khóa công khai y từ x và các tham số hệ thống $\{p,g\}$ là một việc hoàn toàn dễ dàng. Nhưng điều ngược lại thì rất khó thực hiện, nghĩa là từ y và $\{p,g\}$ thì việc tính được khóa bí mật x là không khả thi trong các ứng dụng thực tế. Cần chú ý rằng, theo [5] và [6] để bài toán logarit rời rạc là khó thì p cần phải được chọn đủ lớn với: $|p| \geq 512$ bit.

2. Lược đồ cơ sở

Lược đồ cơ sở ở đây - ký hiệu MTA 16.5 – 01 là một lược đồ chữ ký số bao gồm các thủ tục hình thành tham số và khóa, thủ tục hình thành chữ ký và thủ tục xác minh chữ ký như sau:

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

Thủ tục bao gồm các bước như sau:

1. Sinh 2 số nguyên tố lớn và mạnh: p và q, sao cho: $q \mid (p-1)$ hay: $p = N \times q + 1$, với N là một số nguyên dương.
2. Chọn $g = \alpha^{(p-1)/q} \bmod p$, là phần tử sinh có bậc q của nhóm Z_p^*, ở đây: $\alpha \in Z_p^*$.
3. Khóa riêng x được hình thành bằng cách chọn số nguyên thỏa mãn: $1 < x < q$.

4. Khóa công khai được tính theo công thức:

$$y = g^x \bmod p \tag{1.1}$$

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

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

b) Thủ tục hình thành chữ ký

Dữ liệu đầu vào bao gồm khóa bí mật *x* của người ký và bản tin cần ký M. Thủ tục bao gồm các bước như sau:

1. Chọn ngẫu nhiên một giá trị *k* thỏa mãn: $1 < k < q$, tính giá trị *R* theo công thức:

$$R = g^k \bmod p \tag{1.2}$$

2. Tính thành phần *E* theo công thức:

$$E = H(M \parallel R) \bmod q \tag{1.3}$$

3. Tính thành phần *S* theo công thức:

$$S = x^{-1} \times (k + E) \bmod q \tag{1.4}$$

Chú ý:

- Chữ ký do lược đồ tạo ra với bản tin M ở đây là cặp (*E*,*S*).
- Toán tử "||" sử dụng trong (1.3) là phép ghép nối 2 xâu ký tự/bit.

c) Thủ tục xác minh tính hợp lệ của chữ ký

Dữ liệu đầu vào bao gồm khóa công khai *y* của người ký và bản tin cần thẩm tra M. Thủ tục bao gồm các bước như sau:

1. Tính giá trị *U* theo công thức:

$$U = g^{-E} \times (y)^S \bmod p \tag{1.5}$$

2. Tính giá trị *V* theo công thức:

$$V = H(M \parallel U) \bmod q \tag{1.6}$$

3. Kiểm tra nếu $V = E$ thì chữ ký (E, S) hợp lệ và bản tin M được công nhận về nguồn gốc và tính toàn vẹn.

d) Tính đúng đắn của lược đồ MTA 16.5 – 01

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: $q < n < p$, $1 < x, k < q$, $y = g^x \bmod p$, $R = g^k \bmod p$, $E = H(M \parallel R) \bmod q$, $S = x^{-1} \times (k + E) \bmod q$. Nếu: $U = g^{-E} \times y^S \bmod p$ và $V = H(M \parallel U) \bmod q$ thì: $V = E$.

III. THẬT VẬY, TỪ (1.1), (1.3), (1.4) VÀ (1.5) TA CÓ:

$$\begin{aligned} U &= g^{-E} \times y^S \bmod p = g^{-E} \times g^{x.x^{-1}.(k+E)} \bmod p \\ &= g^{-E+k+E} \bmod p = g^k \bmod p \end{aligned} \tag{1.7}$$

Từ (1.2) và (1.7), suy ra: $U = R$ (1.8)

Thay (1.8) vào (1.6) ta được:

$$V = H(M \parallel U) \bmod q = H(M \parallel R) \bmod q \tag{1.9}$$

Từ (1.3) và (1.9), suy ra: $V = E$

Đây là điều cần chứng minh.

a) Mức độ an toàn của lược đồ MTA 16.5 – 01

Mức độ an toàn của một lược đồ chữ ký số nói chung được đánh giá qua các khả năng:

- Chống tấn công làm lộ khóa mật.
- Chống tấn công giả mạo chữ ký.

Về khả năng chống tấn công làm lộ khóa mật: Từ (1.1) cho thấy mức độ an toàn xét theo khả năng chống tấn công làm lộ khóa mật của thuật toán cơ sở phụ thuộc vào mức độ khó giải của bài toán logarit rời rạc. Cần chú ý rằng,

để bài toán DLP là khó thì các tham số {*p,q,g*} có thể được lựa chọn tương tự như DSA [5] hay GOST R34.10-94 [6], với: $|p| \geq 512bit$, $|q| \geq 160bit$. Ngoài ra, giá trị *k* cũng không được phép sử dụng lại ở các lần ký khác nhau nhằm ngăn chặn khả năng tấn công khóa mật từ (1.4) trong thủ tục hình thành chữ ký của lược đồ.

Về khả năng chống tấn công giả mạo chữ ký: Từ (1.3), (1.5) và (1.6) của thuật toán cơ sở cho thấy, một cặp (*E*,*S*) bất kỳ sẽ được công nhận là chữ ký hợp lệ của đối tượng sở hữu khóa công khai *y* lên bản tin M nếu thỏa mãn điều kiện:

$$E = H((g^{-E} \times y^{S} \bmod p) \| M) \bmod q \tag{1.10}$$

Có thể thấy rằng việc tìm được một cặp (*E*,*S*) giả mạo thỏa mãn (1.10) là một dạng bài toán khó chưa có lời giải nếu các tham số {*p,q,n*} được chọn đủ lớn để phương pháp "*vét cạn*" (*Brute force*) là không khả thi trong các ứng dụng thực tế.

B. Xây dựng thuật toán mật mã khóa công khai

Mục này đề xuất xây dựng 2 dạng thuật toán khác nhau. Để phù hợp với các ứng dụng thực tế, dạng thứ nhất được thiết kế với giả thiết rằng 2 đối tượng A và B tham gia quá trình trao đổi thông tin bí mật theo các bước như sau:

- B yêu cầu A gửi cho mình một bản tin M.
- A kiểm tra yêu cầu nhận được, nếu đúng là B yêu cầu, A sẽ tạo dấu xác nhận của mình lên M và mã hóa bản tin M rồi gửi cho B.
- B giải mã bản tin nhận được, kiểm tra tính hợp lệ của dấu xác nhận do A tạo với bản tin nhận được, nếu dấu xác nhận hợp lệ thì khẳng định bản tin nhận được chính là bản tin M mà B yêu cầu từ A.

Dạng thứ nhất có thể sử dụng phù hợp trong những trường hợp mà ở đó vai trò của A và B là ngang nhau, bên gửi chỉ đáp ứng khi bên nhận yêu cầu trước. Cũng có thể coi yêu cầu của B là sự cho phép bên gửi (A) mã hóa bản tin trong những trường hợp B có mức độ ưu tiên cao hơn.

Ở dạng thứ hai, quá trình trao đổi thông tin giữa 2 đối tượng A và B được giả thiết như sau:

- A mã hóa bản tin M, đồng thời tạo dấu xác nhận bản tin M rồi gửi cho B.
- B giải mã bản tin nhận được và kiểm tra tính hợp lệ của dấu xác nhận mà A tạo ra với bản tin nhận được, nếu dấu xác nhận của A hợp lệ B sẽ tạo và gửi một thông báo xác nhận của mình tới A.
- A kiểm tra thông báo xác nhận của B để biết bản tin M đã được gửi an toàn đến B.

Dạng thứ hai có thể được sử dụng trong những trường hợp vai trò của bên gửi cao hơn, A có thể gửi bản tin bất cứ khi nào cần và B phải có trách nhiệm phản hồi thông báo xác nhận để A biết quá trình trao đổi thông tin đã hoàn tất.

Trong cả 2 dạng thuật toán này, lược đồ chữ ký cơ sở MTA 16.5 – 01 được sử dụng để tạo và kiểm tra dấu xác nhận của A cũng như thông báo xác nhận của B.

1. Thuật toán MTA 16.5 – 02

Thuật toán thứ nhất – ký hiệu MTA 16.5 – 02, được đề xuất ở đây bao gồm thủ tục hình thành tham số hệ thống tương tự như lược đồ cơ sở MTA 16.5 – 01, trong đó khóa bí mật của A và B là x_A và x_B, các khóa công khai tương ứng y_A và y_B được tính theo:

$$y_A = g^{x_A} \bmod p,\ y_B = g^{x_B} \bmod p \tag{2.1}$$

IV. VÀ CÁC THỦ TỤC YÊU CẦU, THỦ TỤC MÃ HÓA VÀ GIẢI MÃ NHƯ SAU:

a) Thủ tục yêu cầu: Được thực hiện bởi đối tượng B, bao gồm các bước như sau:

1. Tạo bản tin yêu cầu A: $M_B = \{ID_B, RQ, T_1, ...\}$ trong đó: ID_B là định danh của B, RQ là yêu cầu về bản tin M và T_1 là nhãn thời gian,...
2. Chọn ngẫu nhiên một giá trị k_B thỏa mãn: $1 < k_B < q$, tính giá trị R_B theo công thức:

$$R_B = g^{k_B} \bmod p \tag{2.2}$$

3. Tính thành phần E_B theo công thức:

$$E_B = H(M_B \| R_B) \bmod q \tag{2.3}$$

4. Tính thành phần S_B theo công thức:

$$S_B = (x_B)^{-1} \times (k_B + E_B) \bmod q \tag{2.4}$$

5. Gửi (M_B,E_B,S_B) cho đối tượng A.

b) Thủ tục mã hóa: Được thực hiện bởi A, bao gồm các bước như sau:

1. Tính giá trị $\overline{R}_B$ theo công thức:

$$\overline{R}_B = g^{-E_B} \times (y_B)^{S_B} \bmod p \tag{2.5}$$

2. Tính giá trị $\overline{E}_B$ theo công thức:

$$\overline{E}_B = H(M_B \parallel \overline{R}_B) \bmod q \tag{2.6}$$

3. Kiểm tra nếu $\overline{E}_B = E_B$ thì (E_B,S_B) là hợp lệ và M_B là do B tạo ra để yêu cầu A gửi bản tin M. Khi đó A sẽ ký lên và mã hóa bản tin M rồi gửi cho B theo các bước sau:

4. Chọn ngẫu nhiên một giá trị k_A thỏa mãn: $1 < k_A < q$, tính giá trị R_A theo công thức:

$$R_A = g^{k_A} \bmod p \tag{2.7}$$

5. Tính thành phần thứ nhất của chữ ký:

$$E_A = H(M \parallel R_A) \bmod q \tag{2.8}$$

6. Tính thành phần thứ 2 của chữ ký:

$$S_A = (x_A)^{-1} \times (k_A + E_A) \bmod q \tag{2.9}$$

7. Tính bản mã C:

$$C = M \times (\overline{R}_B)^{k_A} \bmod p \tag{2.10}$$

8. Gửi (C,E_A,S_A) cho B.

c) Thủ tục giải mã: Được thực hiện bởi B, bao gồm các bước như sau:

1. Tính giá trị $\overline{R}_A$ theo công thức:

$$\overline{R}_A = g^{-E_A} \times (y_A)^{S_A} \bmod p \tag{2.11}$$

2. Giải mã bản tin nhận được:

$$\overline{M} = C \times (\overline{R}_A)^{-k_B} \bmod p \tag{2.12}$$

3. Tính giá trị $\overline{E}_A$ theo công thức:

$$\overline{E}_A = H(\overline{M} \parallel \overline{R}_A) \bmod q \tag{2.13}$$

4. Kiểm tra nếu $\overline{E}_A = E_A$ thì khẳng định (E_A,S_A) là chữ ký hợp lệ của A và : $\overline{M} = M$.

d) Tính đúng đắn của MTA 16.5 – 02

Điều cần chứng minh ở đây là: Cho: p, q là 2 số nguyên tố thỏa mãn: $q \mid (p-1)$, $1 < \alpha < p$, $g = \alpha^{(p-1)/q} \bmod p$, $H : \{0,1\}^* \mapsto Z_n$ với: $q < n < p$, $1 < x_A, x_B < q$, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$, $1 < k_A, k_B < q$, $0 \le M \le p-1$, $M_B = \{ID_B, RQ, T_1, ...\}$, $R_B = g^{k_B} \bmod p$, $R_A = g^{k_A} \bmod p$, $E_B = H(M_B \parallel R_B) \bmod q$, $E_A = H(M \parallel R_A) \bmod q$, $S_B = (x_B)^{-1} \times (k_B + E_B) \bmod q$, $S_A = (x_A)^{-1} \times (k_A + E_A) \bmod q$, $C = M \times (\overline{R}_B)^{k_A} \bmod p$. Nếu: $\overline{R}_B = g^{-E_B} \times (y_B)^{S_B} \bmod p$, $\overline{E}_B = H(M_B \parallel \overline{R}_B) \bmod q$ thì: $\overline{E}_B = E_B$, và nếu: $\overline{R}_A = g^{-E_A} \times (y_A)^{S_A} \bmod p$, $\overline{M} = C \times (\overline{R}_A)^{-k_B} \bmod p$, $\overline{E}_A = H(\overline{M} \parallel \overline{R}_A) \bmod q$ thì: $\overline{E}_A = E_A$ và $\overline{M} = M$.

Chứng minh:

V. THẬT VẬY, từ (2.1), (2.3), (2.4) và (2.5) ta có:

$$\begin{aligned} \overline{R}_B &= g^{-E_B} \times (y_B)^{S_B} \bmod p = g^{-E_B} \times g^{x_B \cdot (x_B)^{-1} \cdot (k_B + E_B)} \bmod p \\ &= g^{-E_B + k_B + E_B} \bmod p = g^{k_B} \bmod p \end{aligned} \tag{2.14}$$

Từ (2.2) và (2.14), suy ra: $\overline{R}_B = R_B$ (2.15)

Thay (2.15) vào (2.6) ta được:

$$\overline{E}_B = H(M_B \parallel \overline{R}_B) \bmod q = H(M_B \parallel R_B) \bmod q \tag{2.16}$$

Từ (2.8) và (2.16), suy ra điều cần chứng minh: $\overline{E}_B = E_B$.

Từ (2.1) và (2.9), ta có:

$$\overline{R}_A = g^{-E_A} \times (y_A)^{S_A} \bmod p = g^{-E_A} \times g^{x_A.(x_A)^{-1}.(k_A+E_A)} \bmod p = g^{-E_A+k_A+E_A} \bmod p = g^{k_A} \bmod p \quad (2.17)$$

Thay (2.10), (2.14) và (2.17) vào (2.12) ta có điều cần chứng minh:

$$\overline{M} = C \times (\overline{R}_A)^{-k_B} \bmod p = \left(M \times (\overline{R}_B)^{k_A} \bmod p\right) \times \left(g^{k_A} \bmod p\right)^{-k_B} \bmod p \quad (2.18)$$
$$= M \times g^{k_A.k_B} \times g^{-k_A.k_B} \bmod p = M$$

Mặt khác, từ (2.2) và (2.17) suy ra: $\overline{R}_A = R_A$ (2.19)

Thay (2.18) và (2.19) vào (2.13) ta được:

$$\overline{E}_A = H(\overline{M} \parallel \overline{R}_A) \bmod q = H(M \parallel R_A) \bmod q \quad (2.20)$$

Từ (2.8) và (2.20) suy ra điều cần chứng minh: $\overline{E}_A = E_A$.

a) Mức độ an toàn của MTA 16.5 – 02

Độ an toàn về khả năng bảo mật thông tin được mã hóa: Từ (2.10) và (2.12) cho thấy một kẻ thứ 3 không mong muốn nào đó (C) có thể giải mã được bản tin nếu tính được giá trị: $g^{k_A.k_B} \bmod p$. Những gì mà C có được ở đây là: $g^{k_A} \bmod p$ và $g^{k_B} \bmod p$. Về lý thuyết , có thể có cách sử dụng tri thức về $g^{k_A} \bmod p$ và $g^{k_B} \bmod p$ để tính $g^{k_A.k_B} \bmod p$. Nhưng hiện tại, chưa có cách nào để tính mà không phải giải bài toán DLP.

Độ an toàn về khả năng chống tấn công giả mạo: Thuật toán được thiết kế dưới dạng một giao thức, các thủ tục mã hóa và giải mã chỉ được thực hiện khi danh tính của A, B và yêu cầu về việc trao đổi thông tin giữa 2 đối tượng được xác thực. Việc xác thực được thực hiện bằng lược đồ chữ ký MTA 16.5 – 01, như vậy độ an toàn của thuật toán xét theo khả năng chống tấn công giả mạo được quyết định bởi mức độ an toàn của lược đồ cơ sở MTA 16.5 – 01.

2. Thuật toán MTA 16.5 – 03

VI. THUẬT TOÁN THỨ HAI – KÝ HIỆU MTA 16.5 – 03, THỦ TỤC HÌNH THÀNH THAM SỐ HỆ THỐNG VÀ KHÓA TƯƠNG TỰ NHƯ MTA 16.5 – 02, THUẬT TOÁN BAO GỒM CÁC THỦ TỤC MÃ HÓA, GIẢI MÃ VÀ THỦ TỤC KIỂM TRA THÔNG BÁO XÁC NHẬN NHƯ SAU:

a) Thủ tục mã hóa: được thực hiện bởi A, bao gồm các bước sau:

1. Chọn ngẫu nhiên một giá trị k_A thỏa mãn: $1 < k_A < q$, tính giá trị R_A theo công thức:

$$R_A = g^{k_A} \bmod p \quad (3.1)$$

2. Tính thành phần thứ nhất của chữ ký:

$$E_A = H(M \parallel R_A) \bmod q \quad (3.2)$$

3. Tính thành phần thứ 2 của chữ ký:

$$S_A = (x_A)^{-1} \times (k_A + E_A) \bmod q \quad (3.3)$$

4. Tính bản mã C:

$$C = M \times (y_B)^{k_A} \bmod p \quad (3.4)$$

5. Gửi (C,E_A,S_A) cho B.

b) Thủ tục giải mã: được thực hiện bởi B, bao gồm các bước sau:

1. Tính giá trị $\overline{R}_A$ theo công thức:

$$\overline{R}_A = g^{-E_A} \times (y_A)^{S_A} \bmod p \quad (3.5)$$

2. Giải mã bản tin nhận được:

$$\overline{M} = C \times (\overline{R}_A)^{-x_B} \bmod p \quad (3.6)$$

3. Tính giá trị $\overline{E}_A$ theo công thức:

$$\overline{E}_A = H(\overline{M} \parallel \overline{R}_A) \bmod q \quad (3.7)$$

4. Kiểm tra nếu $\overline{E}_A = E_A$ thì khẳng định (E_A,S_A) là chữ ký hợp lệ của A và : $\overline{M} = M$. B tạo thông báo xác nhận: $M_B = \{ID_B, ACK, T_2, ...\}$, trong đó: ID_B là định danh của B, ACK là nội dung xác nhận về bản tin M và T_2 là nhãn thời gian,... Sau đó B ký lên thông báo xác nhận này rồi gửi cho A theo các bước sau:

5. Chọn ngẫu nhiên một giá trị k_B thỏa mãn: $1 < k_B < q$, tính giá trị R_B theo công thức:

$$R_B = g^{k_B} \bmod p \tag{3.8}$$

6. Tính thành phần E_B theo công thức:

$$E_B = H(\overline{M} \parallel M_B \parallel R_B) \bmod q \tag{3.9}$$

7. Tính thành phần S_B theo công thức:

$$S_B = (x_B)^{-1} \times (k_B + E_B) \bmod q \tag{3.10}$$

8. Gửi (M_B,E_B,S_B) cho đối tượng A.

c) Thủ tục kiểm tra thông báo xác nhận của B: được thực hiện bởi A, bao gồm các bước sau:

1. Tính giá trị $\overline{R}_B$ theo công thức:

$$\overline{R}_B = g^{-E_B} \times (y_B)^{S_B} \bmod p \tag{3.11}$$

2. Tính giá trị $\overline{E}_B$ theo công thức:

$$\overline{E}_B = H(M \parallel M_B \parallel \overline{R}_B) \bmod q \tag{3.12}$$

3. Kiểm tra nếu $\overline{E}_B = E_B$ thì thì (E_B,S_B) là hợp lệ và B đã nhận đúng bản tin M.

d) Tính đúng đắn của MTA 16.5 – 03

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: $q < n < p$, $1 < x_A, x_B < q$, $y_A = g^{x_A} \bmod p$, $y_B = g^{x_B} \bmod p$, $1 < k_A, k_B < q$, $0 \le M \le p-1$, $R_A = g^{k_A} \bmod p$, $E_A = H(M \parallel R_A) \bmod q$, $S_A = (x_A)^{-1} \times (k_A + E_A) \bmod q$, $C = M \times (y_B)^{k_A} \bmod p$, $M_B = \{ID_B, ACK, T_2, ...\}$, $R_B = g^{k_B} \bmod p$, $E_B = H(M_B \parallel R_B) \bmod q$, $S_B = (x_B)^{-1} \times (k_B + E_B) \bmod q$. Nếu: $\overline{R}_A = g^{-E_A} \times (y_A)^{S_A} \bmod p$, $\overline{M} = C \times (\overline{R}_A)^{-x_B} \bmod p$, $\overline{E}_A = H(\overline{M} \parallel \overline{R}_A) \bmod q$ thì: $\overline{E}_A = E_A$ và $\overline{M} = M$, và nếu: $\overline{R}_B = g^{-E_B} \times (y_B)^{S_B} \bmod p$, $\overline{E}_B = H(M_B \parallel \overline{R}_B) \bmod q$ thì: $\overline{E}_B = E_B$.

Chứng minh:

Từ (2.1) và (3.3), ta có:

$$\overline{R}_A = g^{-E_A} \times (y_A)^{S_A} \bmod p = g^{-E_A} \times g^{x_A \cdot (x_A)^{-1} \cdot (k_A + E_A)} \bmod p = g^{-E_A + k_A + E_A} \bmod p = g^{k_A} \bmod p \tag{3.13}$$

Thay (2.1), (3.4) và (3.13) vào (3.6) ta có điều cần chứng minh:

$$\begin{aligned} \overline{M} &= C \times (\overline{R}_A)^{-x_B} \bmod p = \left(M \times (y_B)^{k_A} \bmod p\right) \times \left(g^{k_A} \bmod p\right)^{-x_B} \bmod p \\ &= M \times g^{k_A \cdot x_B} \times g^{-k_A \cdot x_B} \bmod p = M \end{aligned} \tag{3.14}$$

Mặt khác, từ (3.1) và (3.13) suy ra: $\overline{R}_A = R_A$ (3.15)

Thay (3.14) và (3.15) vào (3.7) ta được:

$$\overline{E}_A = H(\overline{M} \parallel \overline{R}_A) \bmod q = H(M \parallel R_A) \bmod q \tag{3.16}$$

Từ (3.2) và (3.16) suy ra điều cần chứng minh: $\overline{E}_A = E_A$

VII. TỪ (2.1) VÀ (3.10), TA CÓ:

$$\begin{aligned} \overline{R}_B &= g^{-E_B} \times (y_B)^{S_B} \bmod p = g^{-E_B} \times g^{x_B \cdot (x_B)^{-1} \cdot (k_B + E_B)} \bmod p \\ &= g^{-E_B + k_B + E_B} \bmod p = g^{k_B} \bmod p \end{aligned} \tag{3.17}$$

Từ (3.8) và (3.17), suy ra: $\overline{R}_B = R_B$ (3.18)

Thay (3.18) vào (3.12) ta được:

$$\overline{E}_B = H(M_B \parallel \overline{R}_B) \bmod q = H(M_B \parallel R_B) \bmod q \tag{3.19}$$

Từ (3.9) và (3.19), suy ra điều cần chứng minh: $\overline{E}_B = E_B$.

e) Mức độ an toàn của MTA 16.5 – 03

Độ an toàn về khả năng bảo mật thông tin được mã hóa: Từ (3.4) và (3.6) cho thấy C chỉ giải mã được bản tin nếu tính được: $g^{k_A \cdot x_B} \bmod p$ từ : $g^{k_A} \bmod p$ và $g^{x_B} \bmod p$. Như vậy, C cũng không có cách nào để tính $g^{k_A \cdot x_B} \bmod p$ ngoài việc giải bài toán DLP.

Độ an toàn về khả năng chống tấn công giả mạo: Tương tự như thuật toán MTA 16.5 – 02, độ an toàn của thuật toán đề xuất ở đây xét theo khả năng chống tấn công giả mạo cũng được quyết định bởi mức độ an toàn của lược đồ cơ sở MTA 16.5 – 01.

VIII. KẾT LUẬN

Bài báo đề xuất xây dựng 2 thuật toán mật mã khóa công khai dựa trên tính khó của bài toán logarit rời rạc. Các thuật toán đề xuất ở đây được thiết kế dưới dạng giao thức để phù hợp với các ứng dụng trong thực tế. Hơn nữa, các thuật toán này còn có cơ chế xác thực nguồn gốc và tính toàn vẹn của bản tin được mã hóa vì thế có thể chống lại các dạng tấn công giả mạo đã được biết đến trong thực tế.

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] Luu Hong Dung, Le Dinh Son, Ho Nhat Quang, Nguyen Duc Thuy, **"**Developing digital signature schemes based on discrete logarithm problem", Hội nghị khoa học Quốc gia lần thứ VIII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR 2015). ISBN: 978-604-913-397-8, 2015.

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

[6] 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).

DEVELOPING SOME PUBLIC-KEY CRYPTOGRAPHIC ALGORITHMS BASED ON DISCRETE LOGARITHM PROBLEM

Luu Hong Dung, Nguyen Duc Thuy, Nguyen Luong Binh, Tong Minh Duc

ABSTRACT*— This paper proposes some public-key cryptographic algorithms based on the difficulty of the discrete logarithm problem. In addition to information security capabilities, the new proposed algorithm has the ability to validate the integrity and origin of the message is confidential.*

Keywords*— Public-key cryptography, public-key cryptographic algorithm, digital signature algorithm, discrete logarithm problem.*