MÃ MẠNG AN TOÀN DỰA TRÊN HAI HỆ MẬT OMURA-MASSEY VÀ ELGAMAL TRÊN VÀNH SỐ

Phạm Long Âu[#], Nguyễn Bình[+], Ngô Đức Thiện[+]

[#] Cục kỹ thuật nghiệp vụ, Bộ Công an

[+] Học viện Công nghệ Bưu chính Viễn thông

Tóm tắt: Mã mạng là một kỹ thuật mạng, nó cho phép các nút tạo ra các gói dữ liệu mới bằng cách kết hợp các gói nhận được. Kỹ thuật này có một số lợi ích như tăng thông lượng, cải thiện độ tin cậy và tăng độ ổn định của mạng. Tuy nhiên, kỹ thuật mã mạng thường không gắn với việc bảo mật thông tin truyền trên mạng. Bài báo này trình bày ý tưởng xây dựng một mô hình mã mạng dựa trên hai hệ mật mã khóa công khai, nhằm tạo ra một mã mạng an toàn (có khả năng bảo mật).

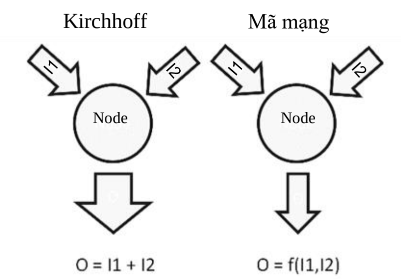
Từ khóa: Mã mạng, vô tuyến hợp tác, hệ mật khóa công khai, bài toán logarit rời rạc, vành số, trường hữu hạn.

I. GIỚI THIỆU

Ngày nay, mã hóa là một phần thiết yếu của bất kỳ hệ thống truyền thông nào. Mã hóa nguồn được sử dụng để nén thông tin ở người gửi để giảm băng thông kênh được sử dụng, khi nhận thành công máy thu có thể giải nén dữ liệu nhận được và lấy thông tin ban đầu. Mã hóa nguồn được gọi là end-to-end vì mã hóa chỉ được thực hiện tại nguồn và giải mã chỉ được thực hiện tại đích.

Bên cạnh đó, mã hóa kênh lại chèn thêm các bit thông tin vào nhằm mục đích sửa sai khi truyền thông tin (bit) qua các môi trường truyền dẫn khác nhau. Thậm chí, mã hóa kênh cũng được coi là end-to-end vì nó được sử dụng trên một tuyến truyền thông duy nhất giữa các nút giao tiếp.

Thời gian gần đây, có thêm một loại mã hóa nữa đó là mã mạng do Ahlswede đề xuất [1]. Từ quan điểm hệ thống, nó không giới hạn ở một lớp cụ thể, nhưng có thể được coi ở lớp ứng dụng, mạng hoặc vật lý. Khác với mã hóa nguồn và kênh, mã mạng không phải mô hình end-to-end, nó cho phép mã hóa đồng thời tại mỗi nút riêng lẻ trong mạng truyền thông. Trong mã hóa mạng, các gói không còn được coi là thực thể hạt nhân của các gói dữ liệu đến và đi của một nút, không nhất thiết phải bằng nhau và các gói riêng lẻ có thể được kết hợp và kết hợp lại tại bất kỳ điểm nào trong mạng. Tính năng mới này có được các lợi thế so với định tuyến trong các mạng lưới truyền thống và cho phép ứng dụng mã hóa mạng trong các lĩnh vực khác nhau.



Hình 1. Sự khác nhau giữa Kirchhoff và mã mạng

Mặt khác, mã hóa mạng cần một cách nhìn mới trên các mạng truyền thông. Hình 1 cho thấy sự khác biệt giữa cách nhìn một nút mạng theo luật Kirchhoff và theo mã mạng. Kirchhoff nói rằng tất cả chảy vào một nút cũng sẽ rời khỏi nút. Với mạng mã một nút có khả năng tạo một đầu ra mới từ các luồng đến. Trong ví dụ đã cho, đầu ra có thể là I1, I2 hoặc kết hợp của cả hai được cho bởi f(I1, I2). Điều quan trọng cần lưu ý là dung lượng của đầu ra sử dụng mã mạng nhỏ hơn tổng dung lượng của dòng vào I1 và I2. Đó là điều sự khác biệt cơ bản đối với các node mạng tiêu chuẩn theo node Kirchhoff.

Thay vì chuyển tiếp các gói tin nhận được theo cách truyền thống, trong mã mạng các node của mạng sẽ kết hợp các gói nhận được và tạo ra các gói mới. Lợi ích của mã mạng làm giảm phiên liên lạc; tối thiểu hóa độ trễ dữ liệu từ nguồn tới đích; tăng độ ổn định của mạng.

Tính năng giảm phiên liên lạc của mã mạng có thể kết hợp với một số hệ mã công khai (mật mã khóa bất đối xứng) để có được một mô hình mã mạng an toàn (có bảo mật). Bài báo này đề xuất sử dụng hai hệ mật khóa công khai Omura-Massey và ElGamal kết hợp với mã mạng. Sau phần Giới thiệu là: phần 2 giới thiệu hai hệ mật khóa công khai; phần 3 đề xuất mô hình mã mạng an toàn; phần 4 là kết luận.

II. HỆ MẬT OMURA - MASSEY VÀ ELGAMAL

A. Bài toán logarit rời rạc

Tác giả liên hệ: Ngô Đức Thiện,
Email: thiennd@ptit.edu.vn
Đến tòa soạn:16/3/2021, chỉnh sửa: 23/6/2021, chấp nhận đăng: 24/7/2021.

Bài toán logarit rời rạc (DLP) là một trong các bài toán một chiều dùng để xây dựng các hệ mật khóa công khai. Phép tính xuôi là hàm lũy thừa rời rạc, thường là phép tính dễ, được dành cho các bên mã hóa và giải mã hợp pháp. Còn phép tính ngược là phép tính logarit rời rạc, là bài toán khó, được dành cho các bên thám mã (giải mã) bất hợp pháp.

Tóm tắt bài toán logarit rời rạc như sau [6]:

Xét một vành số $\mathbb{Z}_p$, nếu p là nguyên tố thì $\mathbb{Z}_p$ là một trường ($\mathbb{Z}_p = GF(p)$). Tập tất cả các phần tử khác 0 của trường sẽ tạo nên một nhóm nhân cyclic $\mathbb{Z}_p^*$.

$$\mathbb{Z}_p^* = \mathbb{Z}_p /\{0\} = \{1,2,\dots,p-1\} \qquad (1)$$

- Cho $g \in \mathbb{Z}_p^*$ là một phần tử sinh (nguyên thủy) của nhóm nhân.

- Cho $y \in \mathbb{Z}_p^*$, yêu cầu hãy tìm x (nếu tồn tại) sao cho: $g^x = y$, tức là: $x = \log_g y$.

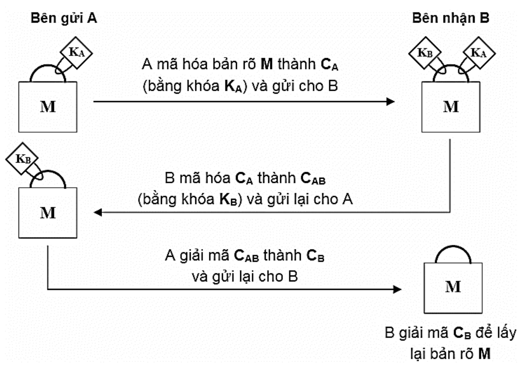
Nhận xét: $\forall y \in \mathbb{Z}_p^*$ thì:

- Bài toán có nghiệm khi g là phần tử nguyên thủy.

- Bài toán có thể không có nghiệm khi g bất kỳ.

B. Hệ mật OMURA – MASSEY

Hệ mật Omura-Massey (O-M) được đề xuất bởi James Massey và Jim. K. Omura lần đầu tiên vào năm 1982 được xem như một cải thiện tích cực trên giao thức Shamir [2], [3].



Hình 2. Minh họa hoạt động của hệ mật O-M

Hoạt động của hệ mật O-M được mô tả như trong hình 1. Hai bên liên lạc A và B sẽ tự tạo cho mình các khóa bảo mật riêng (K_A, K_B), bên A cần gửi bản rõ M cho bên B, quá trình truyền tin thực hiện theo các bước sau:

Bước 1: A mã hóa bản rõ M thành bản mã C_A bằng khóa của A (K_A) và gửi C_A cho B.

Bước 2: B nhận C_A và mã hóa tiếp bằng khóa của B K_B thành bản mã C_{AB} và gửi lại cho A.

Bước 3: A giải mã C_{AB} được C_B rồi gửi lại cho B.

Bước 4: B nhận C_B và giải mã để nhận M.

+ Hệ mật O-M xây dựng trên bài toán DLP

** Tạo khóa*

Khóa công khai: chọn p là một số nguyên tố lớn.

Khóa riêng của A: A chọn cặp số ngẫu nhiên (m, n) thỏa mãn: $m.n \equiv 1\ mod(p-1)$.

Khóa riêng của B: B chọn cặp số ngẫu nhiên (u, v) thỏa mãn: $u.v \equiv 1\ mod(p-1)$.

Chú ý: vì $(m,n),(u,v)$ là các cặp số nghịch đảo nên $m,n,u,v \in \mathbb{Z}_{p-1}^*$, $\mathbb{Z}_{p-1}^*$ là nhóm nhân trên vành số $\mathbb{Z}_{p-1}$. Nhóm nhân này là tập các phần tử là nguyên tố cùng nhau với $(p-1)$, cấu trúc $\mathbb{Z}_{p-1}^*$ như sau:

$$\mathbb{Z}_{p-1}^* = \{i, i < (p-1), \gcd(i, p-1) = 1\} \qquad (2)$$

** Quá trình truyền tin bảo mật*

Bên A muốn gửi một bản rõ M tới bên B.

+ Bước 1: A tính C_A và gửi cho B:

$$C_A = M^m \bmod p \qquad (3)$$

+ Bước 2: B nhận C_A và tính C_{AB} rồi gửi cho A.

$$C_{AB} = (M^m)^u \bmod p \qquad (4)$$

+ Bước 3: A nhận C_{AB} và tính:

$$C_B = (M^{mu})^n \bmod p = M^u \bmod p \qquad (5)$$

và gửi C_B cho bên B.

+ Bước 4: B nhận C_B và giải mã:

$$(M^u)^v \bmod p = M \qquad (6)$$

** Nhận xét*

Để thu được bản rõ thì hệ mật phải có tính lũy đẳng và có tính giao hoán. Với hệ mật O-M các hàm mã hóa và giải mã đều là hàm mũ, với các số mũ là nghịch đảo của nhau nên thỏa mãn.

Việc thám mã hệ mật O-M liên quan tới bài toán logarit rời rạc đây là bài toán khó với số p lớn.

Vì hệ mật O-M không có tính năng xác thực, nên để tránh phép tấn công "Kẻ đứng giữa" (Man in the middle) có thể sử dụng thêm các phương pháp xác thực khác.

C. Hệ mật ElGamal

Hệ mật ElGamal là một hệ mật khóa công khai dựa trên trao đổi khóa Diffie-Hellman, do Taher ElGamal đưa ra vào năm 1985. Mô tả vắn tắt hệ mật như sau [3], [5]:

+ *Tạo khóa*: Bên liên lạc A tạo cho mình một cặp khóa công khai và bí mật, theo các bước sau:

Bước 1: Chọn p là nguyên tố lớn, $g \in \mathbb{Z}_p^*$ là phần tử nguyên thủy.

Bước 2: chọn một số x thỏa mãn $1 < x < p-1$ và tính $g^x\ mod\ p$.

Bước 3: Khóa công khai của A: (p, g, g^x)

Khóa bí mật của A là: x

+ *Mã hóa*: B cần gửi bản tin m cho A ($m < p$)

Bước 1: B nhận khóa công khai của A: (p, g, g^x)

Bước 2: B chọn y ngẫu nhiên $(1 < y < p - 1)$ và tính:

$$\gamma = g^y \bmod p \quad (7)$$

$$\delta = m(g^x)^y \bmod p \quad (8)$$

Bước 3: B gửi bản mã $C = (\gamma, \delta)$ cho A

+ *Giải mã*: A nhận bản mã C và giải mã:

Bước 1: A tính

$$\begin{aligned}\gamma^{-x} &= g^{-xy} \bmod p \\ &= (g^y)^{p-1-x} \bmod p \quad (9)\end{aligned}$$

$$(\gamma^{-x} = \gamma^{p-1-x} \bmod p)$$

Bước 2: A tính

$$\delta.\gamma^{p-1-x} = m.g^{xy}g^{-xy} \bmod p = m \quad (10)$$

+ *Nhận xét*: Để giải mã thì thám mã phải biết x (khóa bí mật) thì phải giải bài toán logarit rời rạc, tức là tính $x = \log_g g^x$) với p lớn không thể giải được, do đó hệ mật là an toàn.

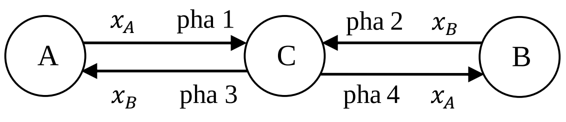
+ Hiệu quả truyền tin thấp, do hệ số mở rộng bản tin $E = 2$ (Bản mã $C = (\gamma, \delta)$ có độ dài bằng 2 lần độ dài bản rõ m).

III. XÂY DỰNG MÃ MẠNG AN TOÀN

A. Mô hình mã mạng đơn giản

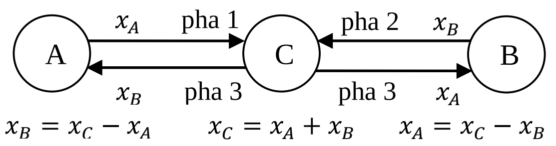
Xét mô hình truyền tin giữa hai nút mạng là A và B. Nếu A và B cách xa nhau, việc truyền thông tin tin cậy rất khó thực hiện được, kể cả khi ta dùng mã kênh.

Trên thực tế, ta có thể đảm bảo việc truyền tin tin cậy giữa A và B bằng cách dùng hệ thống vô tuyến hợp tác (cooperative radio - CR) sử dụng thêm nút chuyển tiếp C (nằm giữa A và B), với quá trình truyền tin được thực hiện như hình 3. Với mô hình này, quá trình truyền tin cần trải qua 4 pha.



Hình 3. Mô hình truyền tin vô tuyến hợp tác

Để tăng hiệu quả của hệ thống CR này, mà vẫn đảm bảo độ tin cậy cần thiết, vào năm 2000 Ahlswede [1] đã đưa ra ý tưởng mã mạng, như hình 4. Theo mô hình này, quá trình truyền tin chỉ còn 3 pha.



Hình 4. Mô hình truyền tin sử dụng mã mạng

Chú ý: các thông tin x_A (của A) cần truyền cho B và x_B (của B) cần truyền cho A được xem là các xâu bit (vector nhị phân n chiều nằm trong không gian tuyến tính n chiều V_n).

Trong mô hình mã mạng hai nút như hình 4, thông tin truyền trên mạng (x_A, x_B, x_C) chưa được bảo mật và xác thực. Bài bào này đề xuất áp dụng hai hệ mật khóa công khai kết hợp với mô hình mã mạng, với mục đích tận dụng ưu điểm của mã mạng và có thêm chức năng xác thực và bảo mật thông tin.

B. Mô hình mã mạng an toàn

Mô hình mã mạng an toàn đề xuất vẫn được xây dựng như hình 4. Giả sử A cần gửi bản tin x_A cho B; Bên B cần gửi bản tin x_B cho A. Quá trình truyền tin theo hai giai đoạn sau:

Giai đoạn 1: Xác thực và truyền tin bảo mật từ A, B đến C, dùng hệ mật ElGamal.

A	**C**	**B**
$x_A \xrightarrow{ElGamal}$	Giải mã lấy lại x_A, x_B và tạo x_C: $x_C = x_A x_B$ (or $x_C = x_A + x_B$)	$\xleftarrow{ElGamal} x_B$

+ A và B dùng khóa công khai của C để mã hóa các bản tin x_A và x_B, sau đó truyền các bản mã cho C.

+ Bên C nhận các bản mã và giải mã để lấy lại x_A, x_B, sau đó kết hợp chúng lại thành bản tin mới x_C.

Giai đoạn 2: Truyền tin bảo mật quảng bá từ C đến A, B bằng hệ mật Omura-Massey.

Bên A	**Bên C**	**Bên B**
	Mã hóa x_C bằng khóa k'_C: $C_C = f(x_C, k'_C)$ và phát quảng bá $\longleftrightarrow$	
Mã hóa C_C bằng k'_A: $C_{C,A} = f(x_C, k'_C, k'_A)$ và gửi $C_{C,A}$ cho C $\longrightarrow$		$\longleftarrow$ Mã hóa C_A bằng k'_B: $C_{C,B} = f(x_C, k'_C, k'_B)$ và gửi $C_{C,B}$ cho C
	Giải mã (gỡ k'_C): $\longleftarrow C_A = f(x_C, k'_A)$ $C_B = f(x_C, k'_B) \longrightarrow$	
+ Giải mã: $x_C = f^{-1}(x_C, k'_A)$ + Tái tạo bản rõ x_B $x_B = x_C x_A^{-1}$ Hoặc $x_B = x_C - x_A$		+ Giải mã: $x_C = f^{-1}(x_C, k'_B)$ + Tái tạo bản rõ x_A $x_A = x_C x_B^{-1}$ Hoặc $x_A = x_C - x_B$

- *Bước 1*:

+ Bên C mã hóa bản tin $x_C \rightarrow C_C = E(x_C, k'_C)$ bằng khóa k'_C của C, rồi phát quảng bá cho A và B.

- *Bước 2*:

+ Bên A nhận C_C mã hóa $C_C \rightarrow C_{C,A}$ bằng khóa k'_A và gửi trả C:

$$C_{C,A} = E(C_C, k'_A) = E(x_C, k'_C, k'_A) \quad (11)$$

+ Bên B nhận C_C mã hóa $C_C \rightarrow C_{C,B}$ bằng khá k'_B và gửi trả C:

$$C_{C,B} = E(C_C, k'_B) = E(x_C, k'_C, k'_B) \quad (12)$$

- *Bước 3*:

+ Bên C nhận $C_{C,A}$ và giải mã $C_{C,A} \rightarrow C_A$ (tháo khóa k'_C), và gửi C_A cho A:

$$C_A = D\left(C_{C,A}, k'_C\right) = E(x_C, k'_A) \quad (13)$$

+ Bên C nhận $C_{C,B}$ và giải mã $C_{C,B} \rightarrow C_B$ (tháo khóa k'_C), và gửi C_B cho B:

$$C_B = D\left(C_{C,B}, k'_C\right) = E(x_C, k'_B) \quad (14)$$

- *Bước 4*:

+ Bên A nhận C_A và giải mã tái tạo bản rõ x_B:

$$x_C = D(C_A, k'_A)$$

$$x_B = x_C . x_A^{-1} \quad (15)$$

+ Bên A nhận C_B và giải mã tái tạo bản rõ x_A:

$$x_C = D(C_B, k'_B)$$

$$x_A = x_C . x_B^{-1} \quad (16)$$

Chú ý: $E(.)$ và $D(.)$ là các hàm mã hóa và giải mã. Để thực hiện mã hóa và giải mã không theo quy tắc "bóc bánh" như biểu thức (13), (14) (tức là có thể thực hiện không theo thứ tự) thì phép mã hóa và giải mã thường phải dựa trên tính chất lũy đẳng của phép tính lũy thừa.

C. Mô hình mã mạng an toàn xây dựng trên bài toán logarit rời rạc

Hoạt động của mã mạng an toàn đề xuất xây dựng trên bài toán DLP thực hiện như sau:

* *Tạo khóa*

+ Tham số chung: Các bên A, B, C chọn:

p - số nguyên tố lớn;

g- phần tử nguyên thủy, $g \in \mathbb{Z}_p^*$;

+ Tham số bí mật: các bên chọn số bí mật như sau:

Bên A:

- Số ngẫu nhiên k_A: $(1 < k_A < p-1)$

- Cặp số: m_A, n_A: $m_A n_A = 1 \; mod \; (p-1)$

Bên B:

- Số ngẫu nhiên k_B: $(1 < k_B < p-1)$

- Cặp số: m_B, n_B: $m_B n_B = 1 \; mod \; (p-1)$

Bên C:

- Số ngẫu nhiên k_C: $(1 < k_C < p-1)$; Tính $g^{k_C} \; mod \; p$ và *công khai* g^{k_C} cho A và B.

- Cặp số: u, v: $uv = 1 \; mod \; (p-1)$

Chú thích: các số bí mật k_A, k_B, k_C sử dụng cho hệ mật ElGamal; các cặp số $(m_A, n_A), (m_B, n_B), (u, v)$ sử dụng cho hệ mật O-M (tương ứng với các khóa k'_A, k'_B, k'_C trong mục *III.B*).

* *Quá trình truyền tin:*

Giai đoạn 1:

+ *Bước 1*: Truyền tin bảo mật từ A, B đến C, dùng hệ mật ElGamal. Bản rõ của A là x_A, và của B là x_B.

Bên A tính (theo (7), (8)):

$$\gamma_A = g^{k_A} \; mod \; p$$

$$\delta_A = x_A (g^{k_C})^{k_A} \; mod \; p$$

và gửi $C_A = (\gamma_A, \delta_A)$ cho C.

Bên B tính:

$$\gamma_B = g^{k_B} \; mod \; p$$

$$\delta_B = x_B (g^{k_C})^{k_B} \; mod \; p$$

và gửi $C_B = (\gamma_B, \delta_B)$ cho C.

Bên C giải mã theo (9), (10):

- Giải mã x_A

$$\gamma_A^{-k_C} = \gamma_A^{p-1-k_C} = g^{-k_A k_C} \; mod \; p$$

$$\gamma_A^{-k_C} \, \delta_A = x_A (g^{k_C k_A}) g^{-k_A k_C} = x_A$$

- Giải mã x_B

$$\gamma_B^{-k_C} = \gamma_B^{p-1-k_C} = g^{-k_B k_C} \; mod \; p$$

$$\gamma_B^{-k_C} \, \delta_B = x_B (g^{k_C k_B}) g^{-k_B k_C} = x_B$$

+ *Bước 2*: Sử dụng kỹ thuật mã mạng: Bên C tạo bản tin x_C từ việc kết hợp các bản tin x_A và x_B, có thể kết hợp theo các cách khác nhau của mã mạng.. Thông thường, có thể thực hiện bằng phép nhân hoặc phép cộng.

- theo phép nhân: $x_C = x_A x_B \; mod \; p$ (17)

- theo phép cộng: $x_C = (x_A + x_B) \; mod \; p$ (18)

Giai đoạn 2: Truyền tin bảo mật quảng bá từ C đến A, B bằng hệ mật Omura-Massey.

+ *Bước 1*: Bên C mã hóa bản tin x_C (theo (3)) và phát quảng bá bản mã cho A, B:

$$C_C = x_C^u \; mod \; p$$

+ *Bước 2*:

Bên A nhận C_C mã hóa $C_C \to C_{C,A}$ (theo (4)) bằng khóa riêng của A và gửi $C_{C,A}$ cho C:

$$C_{C,A} = C_C^{m_A} \, mod \, p = x_C^{u.m_A} \, mod \, p \qquad (19)$$

Bên B nhận C_C mã hóa $C_C \to C_{C,B}$ (theo (4)) bằng khóa riêng của A và gửi $C_{C,B}$ cho C:

$$C_{C,B} = C_C^{m_B} \, mod \, p = x_C^{u.m_B} \, mod \, p \qquad (20)$$

+ *Bước 3*:

Bên C nhận $C_{C,A}$, giải mã $C_{C,A} \to C_A$ (theo (5)) và gửi lại C_A cho A:

$$C_A = C_{C,A}^{v} = x_C^{u.v.m_A} \, mod \, p = x_C^{m_A} \, mod \, p \qquad (21)$$

Bên C nhận $C_{C,B}$, giải mã $C_{C,B} \to C_B$ và gửi lại C_B cho B:

$$C_B = C_{C,B}^{v} = x_C^{u.v.m_B} \, mod \, p = x_C^{m_B} \, mod \, p \qquad (22)$$

+ *Bước 4*:

Bên A nhận C_A và giải mã lấy lại x_C (theo (6))

$$C_A^{n_A} = x_C^{m_A n_A} \, mod \, p = x_C$$

tái tạo bản rõ x_B:

- Theo phép nhân: $x_B = x_C x_A^{-1}$

- Theo phép cộng: $x_B = x_C - x_A$

Bên B nhận C_B và giải mã lấy lại x_C (theo (6))

$$C_B^{n_B} = x_C^{m_B n_B} \, mod \, p = x_C$$

tái tạo bản rõ x_A:

- Theo phép nhân: $x_A = x_C x_B^{-1}$

- Theo phép cộng: $x_A = x_C - x_B$

Ví dụ nhỏ:

* *Tạo khóa*

+ *Tham số chung*: Các bên A, B, C chọn:

$p = 23$ - số nguyên tố;

$g = 5$ là phần tử nguyên thủy, $g \in \mathbb{Z}_{23}^*$;

Bên C: $g^{k_C} = 5^9 mod\ 23 = 11$

($k_C = 9$ là tham số bí mật của C).

+ *Tham số bí mật*:

Bên A chọn:

- Số ngẫu nhiên $k_A = 7$: $(1 < 7 < 30)$

- Cặp số: $(m_A, n_A) = (7,19)$ thỏa mãn:

$$7 \times 19 \, mod \, 22 = 1$$

Bên B chọn:

- Số ngẫu nhiên $k_B = 15 : (1 < 15 < 22)$

- Cặp số: $(m_B, n_B) = (5,9)$ thỏa mãn:

$$5 \times 9 \, mod \, 22 = 1$$

Bên C chọn:

- Số ngẫu nhiên $k_C = 9$: $(1 < 9 < 22)$

- Tính $g^{k_C} = 5^9 mod\ 23 = 11$ *và công khai* g^{k_C} cho A và B (như ở trên).

- Cặp số: $(u, v) = (13,17)$ thỏa mãn:

$$13 \times 19 \, mod \, 22 = 1$$

Tóm lại:

Tham số công khai: $p = 23; g = 5,\ g^9 = 11$

Tham số bí mật:

– Bên A: $k_A = 7; (m_A, n_A) = (7,19)$
– Bên B: $k_B = 15;\ (m_B, n_B) = (5,9)$
– Bên C: $k_C = 9;\ (u, v) = (13,17)$

* *Quá trình truyền tin:*

Giai đoạn 1: Truyền tin bảo mật từ A, B đến C, dùng hệ mật ElGamal.

Giả sử bản rõ của A là $x_A = 3$, và của B là $x_B = 12$.

+ *Bước 1*:

Bên A tính:

$\gamma_A = g^{k_A} = 5^7 mod\ 23 = 17$
$\delta_A = x_A (g^{k_C})^{k_A} = 3.11^7 mod\ 23 = 21$
và gửi $C_A = (17, 21)$ cho C.

Bên B tính:

$\gamma_B = g^{k_B} = 5^{15}\ mod\ 23 = 19$
$\delta_B = x_B (g^{k_C})^{k_B} = 12.11^{15} mod\ 23 = 5$
và gửi $C_B = (19, 5)$ cho C.

Bên C giải mã:

- Giải mã x_A, C tính:

$$\gamma_A^{-k_C} = 17^{-9} = 17^{13} \, mod \, 23 = 10$$

$$\gamma_A^{-k_C} \, \delta_A = 10.21 \text{ mod } 23 = 3 = x_A$$

- Giải mã x_B

$\gamma_B^{-k_C} = 19^{13} \, mod \, 23 = 7$

$$\gamma_B^{-k_C} \, \delta_B = 7.5 \, mod \, 23 = 12 = x_B$$

Chú ý: $\gamma^{-k_C} = \gamma^{p-1-k_C} = \gamma^{22-9}$.

+ *Bước 2*: Bên C kết hợp bản tin theo phép nhân (17):

$$x_C = x_A x_B = 3.12 \; mod \; 23 = 13$$

Giai đoạn 2: Truyền tin bảo mật kết hợp mã mạng.

+ *Bước 1*: Bên C mã hóa bản tin x_C và phát quảng bá bản mã cho A, B:

$$C_C = x_C^u \; mod \; p = 13^{13} \; mod \; 23 = 8$$

+ *Bước 2*:

Bên A nhận $C_C = 8$ và mã hóa $C_C \rightarrow C_{C,A}$, sau đó gửi $C_{C,A}$ cho C (19):

$$C_{C,A} = C_C^{m_A} \; mod \; p = 8^7 \; mod \; 23 = 12$$

Bên B nhận C_C, mã hóa $C_C \rightarrow C_{C,B}$ sau đó gửi $C_{C,B}$ cho C (20):

$$C_{C,B} = C_C^{m_B} \; mod \; p = 8^5 \; mod \; 23 = 16$$

+ *Bước 3*:

Bên C giải mã $C_{C,A} \rightarrow C_A$ (21) và gửi lại C_A cho A:

$$C_A = C_{C,A}^v = 12^{17} \; mod \; 23 = 9$$

Bên C giải mã $C_{C,B} \rightarrow C_B$ (22) và gửi lại C_B cho B:

$$C_B = C_{C,B}^v = 16^{17} \; mod \; 23 = 4$$

+ *Bước 4*:

Bên A nhận C_A và giải mã lấy lại x_C.

$$C_A^{n_A} = 9^{19} \; mod \; 23 = 13$$

tái tạo bản rõ x_B:

$$x_B = x_C x_A^{-1} = 13 * 8 \; mod \; 23 = 12$$

Bên B nhận C_B và giải mã lấy lại x_C.

$$C_B^{n_B} = 4^9 \; mod \; 23 = 13$$

tái tạo bản rõ x_A:

$$x_A = x_C x_B^{-1} = 13 * 2 \; mod \; 23 = 3$$

Chú ý: $3^{-1} mod \; 23 = 8$; $12^{-1} mod \; 23 = 2$ là các cặp số nghịch đảo. Để tính phép lũy thừa các số lớn theo modulo, có thể sử dụng thuật toán bình phương và nhân [2], [4], [7].

IV. KẾT LUẬN

Bài báo đề xuất một mô hình mã mạng kết hợp ưu điểm của mã mạng với các hệ mật mã công khai, để tạo ra một mã mạng an toàn. Các bước của mô hình này tóm tắt như sau: Bước 1: xác thực bảo mật dùng hệ mật ElGamal; bước 2 giải mã và xác thực, kết hợp (che giấu) bản tin bằng mặt nạ cộng hoặc nhân; bước 3 phát quảng bá bằng hệ mật O-M.

Ưu điểm của mô hình đề xuất đó là: (1) Sử dụng được ưu điểm của mã mạng là giảm số phiên truyền dẫn giữa các nút truyền trên mạng (tăng thông lượng), tăng độ ổn định của việc truyền tin; (2) thông tin truyền trong mạng được bảo mật an toàn nhờ các hệ mật khóa công khai. Độ an toàn của các hệ mật khóa công khai dựa trên bài toán logarit rời rạc, đã được chứng minh là bài toán an toàn với trường hợp số nguyên tố lớn.

Tuy nhiên, vì sử dụng hệ mật khóa công khai nên tốc độ mã hóa sẽ không nhanh được như các hệ mật khóa bí mật (đối xứng), do vậy mô hình này chỉ phù hợp cho việc truyền các bản tin ngắn (hoặc truyền khóa).

TÀI LIỆU THAM KHẢO

[1] R. Ahlswede, N. Cai, S. Y. Li & R. Young, "Network information flow. Information theory", *IEEE. Trans on vol IT- 46*, No. 4, pp 1204 - 1216, jul 2000.

[2] D. R. Stinson, "Cryptography Theory and Practice", *CRC Press, 1995*.

[3] Jean-Yves Chouinard - ELG 5373, "Secure Communications and Data Encryption, School of Information Technology and Engineering", *University of Ottawa*, April 2002.

[4] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", *CRC Press*, 1996.

[5] William Stallings "Cryptography and Network Security Principles and Practice", Sixth edition, *Pearson Education*, Inc., 2014.

[6] Frederik Vercauteren, "Discrete Logarithms in Cryptography", *ESAT/COSIC - K.U. Leuven ECRYPT Summer School 2008*.

[7] Rudolf Lidl, Harald Niederreiter, "Finite Fields", *Encylopedia of Mathematics and Its Appliaction*; Volume 20. Section, Algebra, Addison-Wesley Publishing Company, 1983.

SECURE NETWORK CODING BASED ON TWO CRYPTOSYSTEMS OMURA-MASSEY AND ELGAMAL OVER NUMBER RING

Abstract: Network coding is a networking technique that allows nodes to create new data packets by combining received packets. This technique has several benefits such as increased throughput, improved reliability, and increased network stability. However, network coding technology is often do not have the security of information transmitted over the network. This paper presents an idea of building a network coding model based on two public key cryptosystems, in order to create a secure network coding (security capabilities).

Keywords: Network coding, cooperative radio, public key cryptosystem, discrete logarith problem, number ring, finite field.

Phạm Long Âu, Nhận bằng Thạc sĩ năm 2016. Hiện công tác tại Cục Kỹ thuật nghiệp vụ, Bộ Công an. Lĩnh vực nghiên cứu: Lý thuyết thông tin; Lý thuyết mã hóa và mật mã.

Nguyễn Bình, Nhận học vị Tiến sĩ năm 1985, học hàm Giáo sư năm 2006. Hiện đang công tác tại Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu: Lý thuyết thông tin, lý thuyết mã hóa, mật mã

Ngô Đức Thiện, Nhận học vị Tiến sĩ năm 2010. Hiện công tác tại Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu: Lý thuyết thông tin và mã hóa, mật mã.