CMC
UNIVERSITY

RSA ALGORITHMS REPORT

2023

TABLE OF CONTENTS

INTRODUCTION

Hiện tại, dữ liệu được tạo và thu thập trên quy mô lớn từ nhiều nguồn khác nhau, bao gồm thiết bị di động, máy tính cá nhân, máy chủ, cảm biến IoT và hệ thống truyền thông xã hội.

Tuy nhiên, việc quản lý và bảo mật dữ liệu đã trở thành một thách thức đáng kể đối với các tổ chức và cá nhân. Bảo mật dữ liệu ngày càng trở nên quan trọng. Thuật toán RSA là một trong những thuật toán quan trọng để mã hóa thông tin.

RSA là một hệ thống tiền điện tử khóa công khai được phát triển vào năm 1977 bởi Ronald Rivest, Adi Shamir và Leonard Adleman. Thuật toán được đặt tên theo chữ cái đầu tiên của mỗi họ của họ. RSA được sử dụng rộng rãi trong các hệ thống bảo mật thông tin để mã hóa và giải mã dữ liệu.

Thuật toán RSA dựa trên các thuộc tính toán học của các số nguyên tố lớn và độ khó của việc phân tích chúng. Thuật toán sử dụng một cặp khóa, bao gồm khóa công khai và khóa riêng, để mã hóa và giải mã tin nhắn.
Khóa công khai được sử dụng để mã hóa tin nhắn và chỉ chủ sở hữu của khóa riêng tư mới có thể giải mã những tin nhắn đó.
Khóa riêng tư được sử dụng để giải mã tin nhắn và chỉ chủ sở hữu khóa riêng tư mới có thể sở hữu khóa đó.

Thuật toán RSA được coi là một trong những thuật toán mã hóa khóa công khai an toàn và đáng tin cậy nhất, và nó được sử dụng rộng rãi trong nhiều ứng dụng khác nhau, bao gồm mật khẩu email, xác thực truy cập, mã hóa dữ liệu và nhiều hệ thống bảo mật khác.
Trong bài báo cáo này, tôi cung cấp một cái nhìn tổng quan toàn diện về lịch sử, thuộc tính và ứng dụng của thuật toán.

BACKGROUND

Defination - 01

Số chung lớn nhất là số tự nhiên lớn nhất chia cho cả a và b mà không để lại phần còn lại. Từ đồng nghĩa với GCD bao gồm yếu tố chung lớn nhất (GCF), yếu tố chung cao nhất (HCF), ước số chung cao nhất (HCD) và thước đo chung lớn nhất (GCM).

Ước chung lớn nhất thường được viết là gcd(a, b) hoặc, đơn giản hơn, là (a, b), mặc dù ký hiệu sau là mơ hồ, cũng được sử dụng cho các khái niệm như một lý tưởng trong vòng số nguyên, có liên quan chặt chẽ với GCD.

Defination - 02

Số nguyên tố: RSA sử dụng các thuộc tính của số nguyên tố để bảo mật tin nhắn. Các số nguyên tố là các số chỉ có thể chia cho 1 và chính chúng. Tìm số nguyên tố lớn là một bài toán toán quan trọng và khó.

Defination - 03

Hệ số nguyên tố: RSA sử dụng hệ số nguyên tố để tạo khóa công khai và khóa riêng. Hệ số nguyên tố là quá trình tìm các số nguyên tố nhân lên để tạo ra một số tự nhiên

EUCLIDEAN ALGORITHM

Thuật toán Euclide liên tục chia số lớn hơn cho số nhỏ hơn và lấy phần còn lại cho đến khi phần còn lại bằng không.

Tại thời điểm đó, ước chung lớn nhất là phần còn lại khác không cuối cùng. Công thức cho thuật toán Euclid có thể được biểu diễn như sau:

$$GCD(A, B) = GCD(B, A \bmod B)$$
$$\text{IF } B \neq 0 \text{ } GCD(A, 0) = A$$

Ở đây, a mod b biểu thị phần còn lại khi a được chia cho b.

Thuật toán Euclid là một thuật toán đơn giản và hiệu quả để tính ước số chung lớn nhất của hai số nguyên dương.

Định lý nhỏ của Fermat:

Nếu p là một số nguyên tố, thì với các số nguyên bất kỳ a:

$$ap \equiv a \pmod{p}$$

MAIN RESULT

Mô tả ngắn gọn

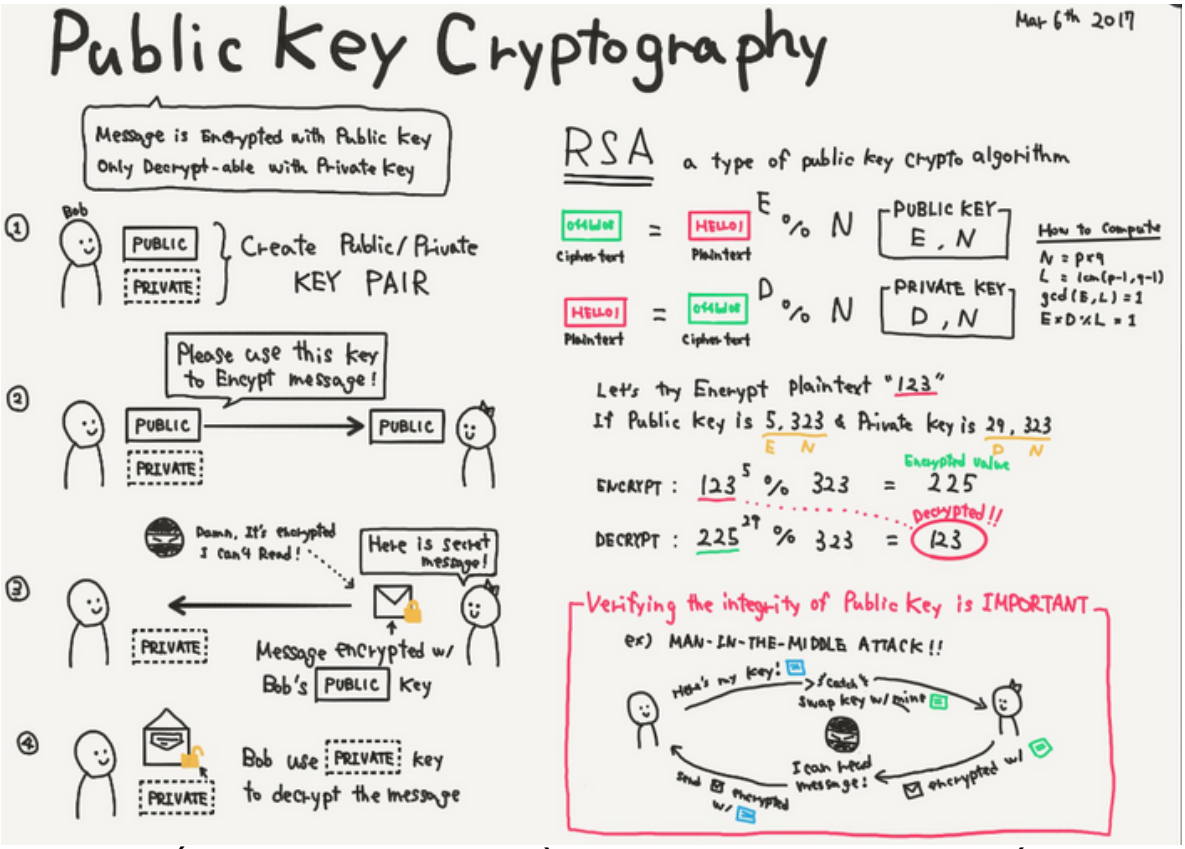
Thuật toán RSA có hai khóa: khóa công khai và khóa riêng tư.

Mỗi khóa là một số cố định được sử dụng trong quá trình mã hóa và giải mã.

Khóa công khai được xuất bản rộng rãi và được sử dụng để mã hóa. Thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa riêng tư tương ứng. Nói cách khác, bất kỳ ai cũng có thể mã hóa nhưng chỉ những người biết khóa riêng tư mới có thể giải mã.

Một sự tương tự trực quan cho một hệ thống mật mã khóa công khai như sau:

B muốn gửi cho A một tin nhắn bí mật mà chỉ A mới có thể đọc. Để làm điều này, A gửi cho B một hộp mở và giữ chìa khóa. B nhận hộp, đặt một chữ cái thông thường bên trong và khóa nó (giống như một khóa thông thường không thể mở một khi đã khóa).



Sau đó, B gửi chiếc hộp trở lại A. A mở hộp bằng chìa khóa của họ và đọc tin nhắn bên trong.

Trong ví dụ này, hộp mở có khóa đóng vai trò là khóa công khai và bản thân khóa là khóa riêng.

HOW TO USED RSA ALGORITHMS?

Here, we already adding a steps explaining your algorithm.

Tạo khoá

STEP 1

Chọn hai số nguyên tố lớn p, q (p ≠q) ngẫu nhiên r và độc lập

100

readers appreciate accurate information

STEP 2

Tính n = pq

100

readers appreciate accurate information

STEP 3

Tính (n) = (p- 1)(q - 1)

STEP 4

Chọn một số nguyên e thỏa mãn 1 < e < (n); e và (n) cùng là số nguyên tố

STEP 5

Tính d thỏa mãn de ≡ e^(-1)(mod (n)).

▪ Khóa công khai

Cặp số được chỉ định n và e tạo thành khóa công khai RSA

▪ Khóa riêng tư

Bao gồm n và d, trong đó d là hàm giải mã và được giữ bí mật.

§ Mã hóa

$$ap \equiv a(\mathrm{mod}\ p)$$

§ Giải mã

$$m = cd \bmod n$$

EXAMPLES

01 — Tạo khoá

Chọn hai số nguyên tố riêng biệt p và q: p = 11 và q = 3.
Tính toán n = p*q: n = 33.
Tính toán (n) = (p-1)(q-1): (n) = 20.
Chọn một số nguyên e sao cho 1 < e < (n) và e là đồng nguyên tố với (n): 7.
Tính số nguyên d sao cho d ≡ e^(-1) (mod (n)): d = 3.
Khóa công khai là (n, e) = (33, 7) và khóa riêng là (n, d) = (33, 3).

02 — Mã hoá

Giả sử chúng ta muốn mã hóa tin nhắn M = 5.
- Chuyển đổi M thành một số m sao cho 0 < m < n: m = 5.
- Tính văn bản mật mã c = m^e (mod n): c = 5^7 (mod 33) =29.

Văn bản mật mã là c = 29.

03 — Giải mã

Để giải mã văn bản mã hóa c = 29, chúng tôi sử dụng khóa riêng (n, d) = (33, 3).
- Tính văn bản thuần túy m = c^d (mod n): m = 29^3 (mod 33) = 5.

Văn bản thuần túy là m = 5, đó là tin nhắn gốc M đã được mã hóa

APPLICATIONS

Giao tiếp an toàn: Thuật toán RSA được sử dụng rộng rãi trong các giao thức giao tiếp an toàn để đảm bảo tính bảo mật và tính toàn vẹn của dữ liệu được truyền qua internet.
Nó được sử dụng trong các giao thức như SSL/TLS, SSH và PGP để mã hóa và giải mã tin nhắn.
Chữ ký số: Thuật toán RSA có thể được sử dụng để tạo chữ ký số, được sử dụng để xác minh tính xác thực và tính toàn vẹn của tài liệu kỹ thuật số. Chữ ký số được tạo ra bằng cách mã hóa thông báo tiêu hóa bằng khóa riêng của người gửi. Người nhận có thể xác minh chữ ký bằng cách giải mã nó bằng khóa công khai của người gửi.
Trao đổi khóa: Thuật toán RSA có thể được sử dụng để trao đổi khóa trong mật mã khóa đối xứng. Hai bên có thể sử dụng thuật toán RSA để trao đổi khóa bí mật được chia sẻ mà không cần truyền nó qua mạng.

CONCLUSION

Tóm lại, RSA là một thuật toán mã hóa khóa công khai được sử dụng rộng rãi và an toàn dựa trên sự khó khăn trong việc bao thanh toán các số nguyên tố lớn. Một trong những điểm mạnh của RSA là nó cung cấp cả tính bảo mật và xác thực. Nó thường được sử dụng để bảo mật dữ liệu nhạy cảm như giao dịch tài chính, giao tiếp trực tuyến và chữ ký số.

HIGHLIGHT 1

- RSA là một thuật toán mã hóa khóa công khai được sử dụng rộng rãi và an toàn dựa trên độ khó của việc bao thanh toán các số nguyên tố lớn.

HIGHLIGHT 2

- Một trong những điểm mạnh của RSA là nó cung cấp cả tính bảo mật và xác thực.
- Nó thường được sử dụng để bảo mật dữ liệu nhạy cảm như giao dịch tài chính, giao tiếp trực tuyến và chữ ký số.

HIGHLIGHT 3

- Tuy nhiên, RSA không hoàn hảo và có một số hạn chế. Một trong những thách thức chính là quy mô chính, cần phải đủ lớn để cung cấp bảo mật đầy đủ.

Ngoài ra, RSA dễ bị tấn công bởi một số cuộc tấn công nhất định như tấn công kênh phụ và tấn công văn bản mật mã đã chọn.
Bất chấp những hạn chế của nó, RSA vẫn là một thuật toán mật mã quan trọng và được sử dụng rộng rãi. Nó đã là công cụ trong việc cho phép giao tiếp an toàn và thương mại điện tử trên internet và có thể sẽ tiếp tục đóng một vai trò quan trọng trong an ninh mạng trong nhiều năm tới.

REFERENCE

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures andpublic-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[2] Stark 1978, p. 16
[3] Rosen, K. H. (2018). Elementary Number Theory and Its Applications (7th ed.).Pearson.
[4] https://en.wikipedia.org/wiki/Euclidean_algorithm#:~:text=In%20mathematics%2C%20the%20Euclidean%20algorithm,them%20both%20without%20a%20remainder.

[5] "Elementary Number Theory" by David M. Burton - This is a popular textbook on numbertheory that covers Fermat's little theorem and other important topics in the field.
[6] https://vi.wikipedia.org/wiki/RSA_(encrytion)

Các tư liệu đã cung cấp thông tin chi tiết về các thuật toán RSA để hỗ trợ trong báo cáo dự án của chúng tôi

Contact

22IT1 - BIT220049

CMC University
84 Nguyen Thanh Binh,
Viet Nam

CMC UNIVERSITY