**Ôn**

|  |  |
| --- | --- |
| **Thuật toán RSA** | |
| **Các bước tính** | **B1**: tính N = p.q  **B2**: tính n=φ=(p-1)(q-1)  **B3**: tìm số e (e là số nguyên tố cùng với n)  **B4**: tìm số d, sao cho e.d ≡1 mod n(d là nghịch đảo của e trong phép modulo)  **B5**: chọn ra mã khóa công khai Ku = (e, N), khóa riêng KR = (d,p,q) |
| **Phương pháp mã hóa bảo mật** | Mã hóa: C = E(M,Ku) = Me mod N  Giải mã: Mngang = D(C,Kr) = Cd mod N |
| **Phương pháp mã hóa chứng thực** | Mã hóa: C = E(M,Kr) = Md mod N  Giải mã: Mngang = D(C,Ku) = Ce mod N |

|  |
| --- |
| **Bảng số nguyên tố** |
| https://tudientoanhoc.com/wp-content/uploads/2019/10/bang-so-nguyen-to-nho-hon-1000-lop-6.jpg |

|  |  |  |
| --- | --- | --- |
| **So Sánh** | **RSA** | **DES** |
| **Loại mã hóa** | Là một thuật toán mã hóa khóa công khai (asymmetric encryption). Nó sử dụng hai khóa: khóa công khai (public key) và khóa bí mật (private key) | Là một thuật toán mã hóa khóa bí mật (symmetric encryption). Nó sử dụng cùng một khóa cho cả quá trình mã hóa và giải mã |
| **Khóa** | Sử dụng cặp khóa, bao gồm khóa công khai (e, n) và khóa bí mật (d, n) | Sử dụng khóa đối xứng (symmetric key) có độ dài 56 bit |
| **Độ dài khóa** | Thường sử dụng độ dài khóa lớn hơn, ví dụ, 2048 bit hoặc 4096 bit, để đảm bảo tính bảo mật cao | Sử dụng khóa có độ dài ngắn hơn, 56 bit, nên có độ bảo mật thấp hơn so với RSA |
| **Tính bảo mật** | RSA được coi là mạnh và an toàn, đặc biệt là với độ dài khóa lớn. Nó phù hợp cho việc bảo vệ khóa và thực hiện ký số | DES đã bị lạc hậu và không còn được coi là an toàn trong nhiều ứng dụng vì độ dài khóa ngắn và các vấn đề liên quan đến quá trình mã hóa |
| **Sử dụng** | Thường được sử dụng cho việc ký số, trao đổi khóa bí mật và mã hóa thông điệp ngắn. Phổ biến trong bảo mật mạng và bảo mật dữ liệu | Thường đã bị thay thế bởi các thuật toán mã hóa đối xứng mạnh hơn như AES (Advanced Encryption Standard) trong nhiều ứng dụng, nhưng vẫn còn được sử dụng trong một số tình huống cụ thể |
| **Số lượng bit cho khóa** | SA thường sử dụng các khóa dài hơn, thường là 1024 bits, 2048 bits hoặc thậm chí 3072 bits để đảm bảo độ an toàn. Với các khóa dài hơn, nó càng an toàn nhưng cũng càng tốn thời gian tính toán | DES sử dụng khóa 56 bits, điều này làm cho nó dễ bị tấn công brute force nếu không sử dụng cơ chế bổ sung |

|  |
| --- |
| **Các bước tạo khóa RSA** |
| B1: Chọn ngẫu nhiên 2 số nguyên tố lớn p và q  B2: Tính số làm modulo của hệ thống: N = p.q  B3: Ta đã biết Ф(N)=(p-1)(q-1) Và có thể dùng Định lý Trung Hoa để giảm bớt tính toán  B4: Chọn ngẫu nhiên khoá mã e trong đó (1<e< ФN), gcd(e, Ф(N))=1 Giải phương trình sau để tìm khoá  B5: giải mã d sao cho e.d=1 mod Ф(N) với 0≤d≤ Ф(N) In khoá mã công khai KU={e, N} Giữ khoá riêng bí mật  KR={d, p, q} |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bảng chữ cái | | | | | | | | | | | | | | | | | | | | | | | | | |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Vd bài mã hóa Ceasar: Sử dụng phương pháp mã hóa đối xứng Ceasar mã hóa bản rõ: "CRYPTOLOGY" với khóa K=5   * **Công thức y=(x+k) mod 26**  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | C | R | Y | P | T | O | L | O | G | Y | | 2 | 17 | 24 | 15 | 19 | 14 | 11 | 14 | 6 | 24 |  |  |  |  | | --- | --- | --- | |  | **Áp dụng công thức: y = (x+k)** | | | **Bản rõ** | **Quy đổi** | **Mã hóa bản rõ** | | C | **(2+5)mod 26=7** | H | | R | **(17+5)mod 26=22** | W | | Y | **(24+5)mod 26=3** | D | | P | **(15+5)mod 26=20** | U | | T | **(19+5)mod 26=24** | Y | | O | **(14+5)mod 26=19** | T | | L | **(11+5)mod 26=16** | Q | | O | **(14+5)mod 26=19** | T | | G | **(6+5)mod 26=11** | L | | Y | **(24+5)mod 26=3** | D |  * HWDUYTQTLD |

|  |
| --- |
| Một số bài tập |
| |  | | --- | | B1: Cho biến đọan mã sau dùng mã Ceasar  "GCUA VQ DTGCM" |  |  | | --- | | B2: Tìm bản mã của bản rõ “We are studying  cryptography this year” sử dụng mã  Playfair với từ khóa “information technology”. |  |  | | --- | | B3: Cho hệ mã Vigenere có M = 6. Giải mã xâu  C = “RANJLV” người ta thu được  bản rõ là “CIPHER”.  a) Tìm khóa đã sử dụng của hệ mã trên.  b) Dùng khóa tìm được ở phần trên hãy hãy giải mã  xâu M = “PLDKCI DUJQJO“ | |

|  |  |
| --- | --- |
| **Một số khái niệm quan trọng** | |
| **Bảo mật thông tin** | Là quá trình bảo vệ thông tin quan trọng khỏi các mối đe dọa và rủi ro, đảm bảo tính bí mật, toàn vẹn và sẵn sàng của thông tin |
| **Các mối đe dọa bảo mật thông tin** | Bao gồm việc xâm nhập hệ thống, phá hoại dữ liệu, lừa đảo, chặn dịch vụ, và nhiều hình thức khác |
| **Toàn vẹn dữ liệu** | Đảm bảo rằng dữ liệu không bị sửa đổi trái phép hoặc thay đổi mà không được phép |
| **Bí mật thông tin** | Bảo vệ thông tin sao cho chỉ những người được ủy quyền mới có thể truy cập và hiểu nó |
| **Sẵn sàng thông tin** | Đảm bảo rằng thông tin luôn sẵn sàng và truy cập được khi cần thiết, đặc biệt trong các tình huống khẩn cấp |
| **Xác thực và ủy quyền** | Xác định xem người dùng hoặc hệ thống có quyền truy cập vào thông tin hay không và xác minh danh tính của họ |
| **Mã hóa** | Sử dụng thuật toán mã hóa để biến đổi thông tin thành dạng không đọc được, tránh việc truy cập trái phép |
| **Mạng bảo mật** | Bảo vệ hệ thống và dữ liệu trên mạng, bao gồm cách thức quản lý truy cập và phân phối thông tin qua mạng |
| **Firewall** | Là một phần mềm hoặc phần cứng giúp kiểm soát và lọc lưu lượng mạng, ngăn chặn các truy cập không ủy quyền |
| **Các chuẩn và quy định bảo mật** | Bao gồm các hướng dẫn và quy tắc được thiết lập để đảm bảo tuân thủ bảo mật thông tin, như ISO 27001, NIST, GDPR, HIPAA, v.v. |
| **Bảo mật vật lý** | Bảo vệ các tài sản vật lý, như máy chủ, phòng máy, hệ thống lưu trữ dữ liệu khỏi truy cập trái phép |
| **Xử lý sự cố bảo mật** | Quy trình xử lý khi có sự cố bảo mật xảy ra, bao gồm phân tích sự cố, khắc phục và báo cáo |
| **Bảo mật ứng dụng:** | Đảm bảo rằng phần mềm và ứng dụng được phát triển và triển khai một cách an toàn |
| **Tấn công mạng** | Các kỹ thuật và phương pháp mà tin tặc sử dụng để tấn công hệ thống, bao gồm hacking, phishing, malware, v.v. |
| **Chính sách bảo mật:** | Quy định và hướng dẫn cụ thể về cách thức bảo mật thông tin trong tổ chức hoặc hệ thống |
| **Mật khẩu (Password)** | Mật khẩu là một chuỗi ký tự hoặc số được sử dụng để xác thực người dùng và truy cập vào tài khoản hoặc hệ thống |
| **Xác thực (Authentication)** | Là quá trình xác định xem một người dùng hoặc thiết bị có quyền truy cập vào hệ thống hay không. |
| **Mật mã (cryptography)** | K/N: Là một khái niệm quan trọng trong môn bảo mật thông tin. Nó liên quan đến việc áp dụng các kỹ thuật và phương pháp để bảo vệ thông tin trước khi truyền đi hoặc lưu trữ, đảm bảo rằng thông tin này chỉ có thể được đọc hoặc hiểu bởi những người có quyền truy cập  Mục tiêu của Mật mã: Mục tiêu chính của mật mã là bảo vệ tính bí mật, tính toàn vẹn và tính xác thực của thông tin. Điều này đảm bảo rằng thông tin không bị tiết lộ cho những người không được ủy quyền, không bị sửa đổi trong quá trình truyền tải, và nguồn gốc của thông tin có thể được xác định.  **Mã hóa (Encryption):** Mã hóa là quá trình biến đổi thông tin gốc thành một dạng không đọc được (ciphertext) bằng cách sử dụng một thuật toán mã hóa và một khóa mã hóa. Để giải mã, người nhận cần sử dụng cùng một khóa mã hóa và thuật toán mã hóa.  **Giải mã (Decryption):** Giải mã là quá trình chuyển đổi ciphertext trở lại thành thông tin gốc sử dụng khóa mã hóa và thuật toán giải mã tương ứng.  **Khóa mã hóa (Encryption Key):** Khóa mã hóa là một chuỗi giá trị được sử dụng trong quá trình mã hóa và giải mã. Có hai loại khóa: khóa công khai và khóa riêng tư. Khóa công khai được chia sẻ rộng rãi và dùng để mã hóa thông tin. Khóa riêng tư được giữ bí mật và dùng để giải mã.  **Mật mã hóa đối xứng và bất đối xứng:** Trong mật mã hóa đối xứng, cùng một khóa được sử dụng cho cả mã hóa và giải mã. Trong mật mã hóa bất đối xứng (asymmetric cryptography), có hai khóa: khóa công khai và khóa riêng tư, và chúng không giống nhau. Loại mật mã hóa này thường được sử dụng trong việc thiết lập kênh liên lạc an toàn.  **Chữ ký số (Digital Signature):** Chữ ký số được sử dụng để xác minh tính xác thực của một thông tin hoặc tài liệu. Nó được tạo ra bằng cách sử dụng khóa riêng tư của người ký và có thể được kiểm tra bằng khóa công khai tương ứng.  **Băm (Hashing):** Băm là quá trình chuyển đổi dữ liệu thành một giá trị băm duy nhất. Giá trị băm này thường được sử dụng để kiểm tra tính toàn vẹn của dữ liệu |
|  |  |