**Bài ôn tập**

**Câu 1:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa Playfair, tìm bản mã tương ứng. Biết keyword là “TINHOC”.

Bản mã là: NPZEIKEBNOTEGNHOOCLXIOQECFTHKILIOARV

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP.

**Câu 2:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa Rail Fence, tìm bản mã tương ứng. Biết số dòng k = 4.

Bản mã là: TDKKTGRGACIEYACNIUNIONTTUOGEOHHHNP

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 3:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa Vigenere, tìm bản mã tương ứng. Biết keyword là “TINHOC”.

Bản mã: MZHVBIWIVOBEPQAOHGDGQOICMKIUUPZVPLD

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 4:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa hàng, tìm bản mã tương ứng. Biết Key = (6 3 2 5 4 1)

Bản mã là:GCEANUINTOIRAIYCHNOTUGPOHHHNETDKKTG

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 5:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa Caesar , tìm bản mã tương ứng. Biết khóa k = 4

Bản mã là: XVYSRK HEMLSG OMRLXI OCXLYE XGSRKR KLMIT

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 6:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa đơn bảng , tìm bản mã tương ứng. Biết khóa k = DKVQFIB JWPESCX HTMYAUO LRGZN tương ứng với bản chữ cái Tiếng Anh.

Bản mã là: UYOHXBQDWJHVEWXJUFEZUJODUVHXBXBJWFT

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 7:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa khóa tự động , tìm bản mã tương ứng. Biết khóa k = BỘ CÔNG THƯƠNG.

Bản mã là: UFWCAMWHCVBIDZHVGKNYBOICDKBUANQFBLV

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 8:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa Affine , tìm bản mã tương ứng. Biết keyword là (11,13).

Mã hóa: OSZLABUNXMLVJTXAMOFTROMZNOJLABABMXFW

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 9:** Cho chuỗi Plaintext P: “TRUONG DAI HOC KINH TE KY THUAT CONG NGHIEP”. Sử dụng hệ mã hóa Hill, tìm bản mã tương ứng. Biết khoá K là:

A number grid with numbers

Description automatically generated

Mã hóa: JOVQQWUFLOAHLBLJBSRCBKLHZZDYGZQHPDYJKW

Giải mã: TRUONGDAIHOCKINHTEKYTHUATCONGNGHIEP

**Câu 10:** Giả sử Alice và Bob muốn trao đổi dữ liệu với nhau bằng phương pháp mã hóa khóa bất đối xứng RSA. Hai bên tự tính khóa của mình và trao đổi khóa công khai cho nhau:

1.Alice chọn p=11, q=3,e=3. Tính KUA và KRA

2.Bob chon p=13, q=11,e=11. Tính KUB và KRB

3.Giả sử Alice muốn gửi bản rõ P=5 cho Bob. Hãy giúp Alice mã hóa P để gửi cho Bob và hãy giúp Bob giải mã C nhận được từ Alice

4.Giả sử Alice tính được H(M)=11 từ một bản tin M, hãy giúp Alice kí vào H(M)

5.Giả sử Bob nhận được bản tin M và chữ kí S được gửi đi từ Alice. Bob cũng tính được H(M)=11. Chứng minh rằng chữ kí S nhận được là của Alice.

Bài làm

**1)** p=11, q=3,e=3

+)Tính n= 11x3= 33

+)Tính Ø(n) = 10x2 = 20

+) Tính d = 3xd mod 20 = 1

* D = 7 vì 3xd mod 20 = 1

**Vậy KUa = {3,33}**

**KRa ={7,33}**

**2)** chon p=13, q=11,e=11

+)Tính n= 13x 11= 143

+)Tính Ø(n) = 12x10 = 120

+) Tính d = 11xd mod 120 = 1

* D = 11 vì 11xd mod 120 = 1

**Vậy KUa = {11,143}**

**KRa ={11,143}**

**3)** Giả sử Alice muốn gửi bản rõ P=5 cho Bob. Hãy giúp Alice mã hóa P để gửi cho Bob và hãy giúp Bob giải mã C nhận được từ Alice

+Mã hóa p= 5

* C= 511mod 143 = 60

+Giải mã C = 60

* P = 6011mod 143 =( 601 x 602 x 608 )mod 143

11= 1+2 +8

+)601 mod 143 = 60

+)602 mod 143 = 25

+)604 mod 143 = 53

+)608 mod 143 = ( 604 x 604 ) mod 143 = 92

* **P= ( 60x25x92) mod 143 = 5**

**4)** Giả sử Alice tính được H(M)=11 từ một bản tin M, hãy giúp Alice kí vào H(M)

**+)Tính s = H(M)d mod 33 = 117 mod 33 = 11**

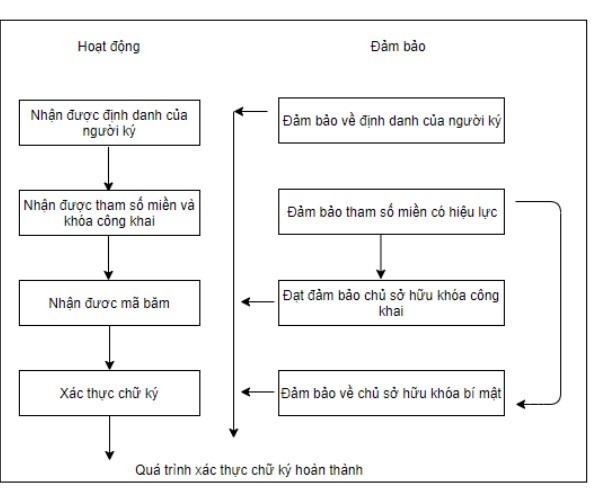
**5)** Giả sử Bob nhận được bản tin M và chữ kí S được gửi đi từ Alice. Bob cũng tính được H(M)=11. Chứng minh rằng chữ kí S nhận được là của Alice.

**+)Tinh H(M) = se mod 33 = 113 mod 33 = 11**

**Vậy S chính là chữ ký nhận được của Bob.**

**Câu hỏi ôn tập lý thuyết**

**Câu 6:** Vẽ sơ đồ và cho biết ý nghĩa các thành phần của hệ thống ký và xác thực chữ ký số.



**Hệ thống ký và xác thực chữ ký số bao gồm các thành phần chính sau đây:**

* Hoạt động
* Nhận được định danh của người ký: Bước này liên quan đến việc xác định danh tính của người ký (người gửi). Đây có thể là một phần của quá trình xác thực danh tính người ký thông qua các chứng chỉ số.
* Nhận được tham số miền và khóa công khai: Sau khi xác định được danh tính của người ký, bước tiếp theo là thu thập các tham số miền (domain parameters) và khóa công khai của người ký. Các tham số miền có thể bao gồm thông tin về thuật toán và các giá trị liên quan đến khóa công khai.
* Nhận được mã băm: Văn bản hoặc thông tin gốc sẽ được băm (hash) để tạo ra một mã băm (message digest). Mã băm này sau đó sẽ được sử dụng trong quá trình xác thực chữ ký.
* Xác thực chữ ký: Bước cuối cùng là xác thực chữ ký số bằng cách sử dụng khóa công khai của người ký để giải mã chữ ký số và so sánh với mã băm của văn bản gốc. Nếu hai mã băm này khớp nhau, chữ ký được xác nhận là hợp lệ.Khóa riêng tư (Private Key): Là phần còn lại của cặp khóa và được giữ bí mật. Nó được sử dụng để giải mã dữ liệu và tạo chữ ký số.
* Đảm bảo
* Đảm bảo về định danh của người ký: Đảm bảo rằng danh tính của người ký là đúng và đã được xác thực. Điều này giúp xác nhận rằng người ký thực sự là người mà họ tuyên bố.
* Đảm bảo tham số miền có hiệu lực: Xác nhận rằng các tham số miền được sử dụng trong quá trình ký và xác thực là hợp lệ và đáng tin cậy. Điều này bao gồm việc kiểm tra tính toàn vẹn và tính chính xác của các tham số.
* Đạt đảm bảo chủ sở hữu khóa công khai: Đảm bảo rằng khóa công khai thực sự thuộc về người ký và có thể được sử dụng để xác thực chữ ký số của họ. Điều này có thể bao gồm việc xác nhận rằng khóa công khai được liên kết với chứng chỉ số của người ký.
* Đảm bảo về chủ sở hữu khóa bí mật: Đảm bảo rằng chỉ người ký mới sở hữu khóa bí mật tương ứng với khóa công khai đã được cung cấp. Điều này giúp xác nhận rằng chữ ký số được tạo ra bởi chính người ký.

**Câu 7:** Hệ thống mật mã khóa đối xứng là hệ thống mật mã khóa bí mật hay khóa công khai? Vì sao?

\* Hệ thống mật mã khóa đối xứng là hệ thống mật mã khóa bí mật. Điều này có nghĩa là cả người mã hóa và người giải mã đều sử dụng cùng một khóa để mã hóa và giải mã thông tin. Vì:

* Trong hệ thống mật mã khóa đối xứng, chỉ có một khóa duy nhất được sử dụng cho cả quá trình mã hóa và giải mã. Khóa này phải được giữ bí mật và chỉ được chia sẻ giữa các bên cần trao đổi thông tin.
* Do chỉ có một khóa duy nhất nên vấn đề bảo mật của hệ thống phụ thuộc rất lớn vào việc bảo vệ khóa này. Nếu khóa bị lộ, kẻ tấn công có thể dễ dàng giải mã thông tin.
* Ví dụ điển hình của hệ thống mật mã khóa đối xứng là AES (Advanced Encryption Standard) và DES (Data Encryption Standard).
* Ngược lại, hệ thống mật mã khóa công khai sử dụng hai khóa khác nhau: một khóa công khai để mã hóa và một khóa bí mật để giải mã. Trong hệ thống này, khóa công khai có thể được chia sẻ tự do, nhưng khóa bí mật phải được giữ kín.

**Câu 8:** Hệ thống mật mã khóa bất đối xứng là hệ thống mật mã khóa bí mật hay khóa công khai? Vì sao?

+Hệ thống mật mã khóa bất đối xứng là hệ thống mật mã khóa công khai.

+ Vì sao:

- Trong hệ thống mật mã khóa bất đối xứng, có hai khóa khác nhau: khóa công khai (public key) và khóa bí mật (private key).

- Khóa công khai được sử dụng để mã hóa thông tin và có thể được chia sẻ tự do với bất kỳ ai.

- Khóa bí mật được sử dụng để giải mã thông tin và phải được giữ kín.

- Vì hai khóa này có mối quan hệ toán học đặc biệt, dữ liệu mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng, và ngược lại.

- Hệ thống này giúp giải quyết vấn đề phân phối khóa an toàn vì khóa công khai không cần được bảo vệ nghiêm ngặt.

- Ví dụ điển hình của hệ thống mật mã khóa bất đối xứng là RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), và ECC (Elliptic Curve Cryptography).

* Do đó, hệ thống mật mã khóa bất đối xứng còn được gọi là hệ thống mật mã khóa công khai vì nó sử dụng một cặp khóa với một khóa công khai được tự do chia sẻ và một khóa bí mật được giữ kín.

**Câu 9:** Vẽ sơ đồ mô hình đảm bảo bí mật? Hãy cho biết KU trong mô hình làm nhiệm vụ gì?

A diagram of a diagram

Description automatically generated

**Sơ đồ mô hình đảm bảo bí mật**

KU (Key Management Unit - Đơn vị quản lý khóa) làm nhiệm vụ:

* Tạo khóa bí mật (Key Generation): KU chịu trách nhiệm tạo ra khóa bí mật (K) được sử dụng cho quá trình mã hóa và giải mã.
* Phân phối khóa (Key Distribution): KU đảm bảo việc phân phối khóa bí mật một cách an toàn giữa các bên tham gia, tức là giữa người gửi (A) và người nhận (B). Việc này rất quan trọng để đảm bảo rằng khóa không bị lộ ra ngoài trong quá trình trao đổi.
* Quản lý khóa (Key Management): KU còn chịu trách nhiệm quản lý vòng đời của khóa, bao gồm lưu trữ, cập nhật, và hủy bỏ khóa khi không còn cần thiết hoặc khi khóa bị lộ.

Hệ thống KU đảm bảo rằng chỉ những người có quyền mới có thể truy cập và sử dụng khóa bí mật, từ đó bảo vệ tính bảo mật của thông tin.

**Câu 10:** Vẽ sơ đồ mô hình đảm bảo bí mật? Hãy cho biết KR trong mô hình làm nhiệm vụ gì?

A diagram of a flowchart

Description automatically generated

KR (Khóa dùng cho mã hóa - Key for encryption) làm nhiệm vụ:

* Mã hóa (Encryption): KR được sử dụng để mã hóa văn bản gốc (Plaintext) thành bản mã (Ciphertext) trước khi gửi đi. Điều này đảm bảo rằng thông tin gửi đi không thể đọc được bởi bất kỳ ai không có khóa giải mã tương ứng.
* Giải mã (Decryption): KR cũng được sử dụng để giải mã bản mã (Ciphertext) thành văn bản gốc (Plaintext) sau khi nhận được. Người nhận sử dụng cùng một khóa KR để chuyển đổi bản mã trở lại dạng nguyên thủy mà chỉ những người có khóa KR mới có thể thực hiện.

Trong hệ thống mật mã khóa đối xứng, cả quá trình mã hóa và giải mã đều sử dụng cùng một khóa, do đó bảo mật của hệ thống phụ thuộc vào việc giữ kín khóa KR. Việc quản lý và bảo vệ khóa này là nhiệm vụ quan trọng để đảm bảo tính bí mật của thông tin trao đổi giữa người gửi và người nhận.