CRITTOGRAFIA

La crittografia è un insieme di procedure ideate allo scopo di nascondere il significato di un messaggio a tutti tranne che al legittimo proprietario.

Requisiti di sicurezza

- **autenticazione**: assicurazione dell'idendità dei soggetti coinvolti nella trasmissione
- **controllo degli accessi**: inibizione dell'uso di una risorsa da parte di soggetti non autorizzati
- **confidenzialità**: protezione della riservatezza dei dati (nessun soggetto terzo deve accedere ai dati dei soggetti coinvolti nella trasmissione)
- **integrità**: assicurazione che i dati non siano stati alterati da soggetti non autorizzati
- **non ripudiabilità**: protezione contro la negazione di un soggetto coinvolto nella comunicazione

Classificazione degli algoritmi in base a:

- **Operazioni**
  - **Sostituzione**: (cesare, Vigenère) ogni elemento del testo in charo è trasformato in un altro elemento
  - **Trasposizione (/permutazione)**: (matrice) gli elementi del testo in chiaro sono riorganizzati
- **Modalità**
  - **a blocchi**: il testo viene diviso in blocchi di N bit (dimensione fissa) ed ogni blocco viene elaborato in modo indipendente dagli altri
  - **a flusso**: elabora un quantitativo di bit variabile, senza una lunghezza predefinita
- **Numero di chiavi**
  - **Simmetrica (1, DES)**: la chiave del mittente e quella del destinatario sono la stessa
  - **Asimmetrica (2, RSA)**: ogni soggetto ha una chiave pubblica ed una privata

DES (Data Encryption Standard)

Algoritmo simmetrico a blocchi

Caratteristiche (Claude Shannon):

- **Confusione**, confondere la relazione tra il testo in chiaro e quello cifrato, tipicamente tramite sostituzione

  Combinare in modo complesso il messaggio e la chiave, per non permettere al crittoanalista di separare le due sequenze mediante l'analisi del crittogramma.

- **Diffusione**, alterare la struttura del testo in chiaro "spargendo" i caratteri su tutto il testo cifrato, tipicamente tramite trasposizione

Input:

- Testo in chiaro suddiviso in blocchi di dimensione fissa pari a 64 bit
- chiave a 56 bit (2^{56} combinazioni), i rimanenti 8 bit sono usati per il controllo di parità

Passaggi:

- **Permutazione iniziale** dei 64 bit di testo in chiaro

  usando una matrice (8*8, valori 1..64) di permutazione casuale

- **Divisione** di ogni blocco in due sottoblocchi (sinistro e destro) da 32 bit

  utilizzati come input della prima iterazione

- Lo **scheduler** utilizza la chiave per generare 16 sottochiavi da 48 bit ciascuna

  usando una matrice (8*7) di permutazione casuale, tramite essa si rimescola e comprime la chiave in input per ottenere in output una chiave da 48 bit

- sequenza di 16 **iterazioni**
  - Ogni iterazione prende due ingressi a 32 bit e produce uscite a 32 bit
  - L'output di sx è semplicemente una copia dell'input di dx
  - L'output di dx consiste nelllo XOR bit per bit dell'input di sx con il risultato della funzione di Feistel dell'input di dx e della chiave K_i di questa iterazione i-ma

    $xor(sx, feistel(rx, K_i))$

    Passaggi della funzione di Feistel:

    - **Espansione**: i 32 bit del blocco di destra vengono espansi in 48 bit mediante una matrice di espansione, semplicemente alcuni bit vengono ripetuti
    - **Miscelazione con la chiave**: viene fatto uno XOR tra i 48 bit ottenuti e la chiave K_i, la sequenza ottenuta viene suddivisa in 8 stringhe da 6 bit
    - **Sostituzione**: queste vengono date in ingresso ad 8 S-BOX ottenendo in uscita 8 stringhe da 4 bit

      il compito delle S-BOX è di compressione per restituire un risultato di 32 bit
    - **Permutazione (?)**: infine, i 32 bit risultanti dalle S-box sono riordinati in base alle permutazioni fisse della P-box o permutation box.

- **Permutazione finale**

  inversa di quella iniziale, utilizzando un'altra matrice di permutazione

- **scambio** i due sottoblocchi (sx e dx) (per predisporre la decifratura)

Si è dimostrata la vulnerabilità del DES nel 1998, l'anno successivo è stato introdotto il **tripleDES (3DES)** che utilizza una chiave di lunghezza tripla (168 bit) per poter operare tre iterazioni del DES consecutive

la sola differenza tra la cifratura e la decifratura è che le sottochiavi sono applicate nell'ordine inverso nella fase di decifratura

RSA

Algoritmo asimmetrico

Si basa sulla difficoltà di fattorizzazione di un numero intero ottenuto dal prodotto di due numeri primi

Key Generation

You need to generate public and private keys before running the functions to generate your ciphertext and plaintext.

They use certain variables and parameters, all of which are explained below:

- Choose two large prime numbers (**p** and **q**)
- Calculate **n** = p*q and **z** = (p-1)(q-1)
- Choose a number **e** where 1 < e < z
- Calculate **d**: e*d mod z = 1

- You can bundle public key pair as (n,e)
- You can bundle private key pair as (n,d)

Encryption/Decryption Function

Once you generate the keys, you pass the parameters to the functions that calculate your ciphertext and plaintext using the respective key.

- If the plaintext is m, ciphertext = me mod n.
- If the ciphertext is c, plaintext = cd mod n

To understand the above steps better, you can take an example where **p**=11 and **q**=3

n = p * q = 33

z = (p-1)(q-1) = 20

Value of **e** can be 7 as it satisfies the condition $1 < e < z$ and not be a factor of n, so they have to be coprimes

d = e * d mod z = 1 7 * d mod 20 = 1 d = 3

Public Key pair = (n,e) = (33,7)

Private Key pair = (n,d) = (33,3)

If the plaintext (m) value is 14 (<n), you can encrypt it using the formula:

m^e mod n = 14^7%33 = 20

To decrypt this ciphertext (c) back to original data, you must use the formula:

c^d mod n = 20^3%33 = 14

You can now look at the factors that make the RSA algorithm stand out versus its competitors in the advantages section.

Si può generare per prima la chiave privata e successivamente quella pubblica siccome sono legate da un rapporto moltiplicazione e godono della proprietà commutativa

Firma digitale

è l'equivalente elettronico della firma autografa su carta, è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta l'integrità, l'autenticità e la non ripudiabilità.

La firma digitale utilizza un certificato digitale rilasciato da un ente certificatore

Algoritmo:

- Dal testo in chiaro viene generato l'hash tramite un funzione one-way (non reversibile)
- l'hash viene crittografato con la chiave privata e viene apposto al documento
- il destinatario potrà generare l'hash del documento e confrontarlo con l'hash cifrato (che viene decifrato con la chiave pubblica), validando identicità (quindi l'identità del mittente)