(EXPORT)Crittografia

La **Crittografia** è la pratica e lo studio delle tecniche di comunicazione per proteggere informazioni sensibili o segrete da letture non autorizzate da terzi.

La crittografia è composta da 3 principali caratteristiche:

- Autenticazione: Si riferisce alla capacità di verificare l'identità del mittente di un messaggio
- Affidabilità: Si riferisce alla capacità di garantire che il messaggio non sia stato modificato da terzi
- Segretezza: Si riferisce alla capacità di mantenere il contenuto di un messaggio privato e non accessibile a persone non autorizzate.

202303240800
Status:
Tags: Sistemi

Autenticazione

Nella Crittografia, l'**Autenticazine*** si riferisce alla **capacità di verificare l'identità del mittente di un messaggio**.
In altre parole, l'autenticazione verifica l'identità del mittente del messaggio.

Un metodo per garantire l'**Autenticazione** di un messaggio è la Firma Digitale o Crittografia Asimmetrica a Chiave Privata.

References

ChatGPT

202303242219
Status:
Tags: Sistemi

Affidabilità

Nella Crittografia, l'**Affidabilità** si riferisce alla capacita di garantire che il messaggio non sia stato modificano in modo non autorizzato da terze parti diverse dal mittente.

Un metodo per garantire l'**Affidabilità** di un messaggio è la Firma Digitale o Crittografia Asimmetrica con Chiave Privata

---

References

ChatGPT

202303242225
Status:
Tags: Sistemi

Segretezza

Nella Crittografia, la **Segretezza** si riferisce alla capacità di mantenere il contenuto di un messaggio privato e non accessibile a persone non autorizzate.
In altre parole, questa garantisce che solo il destinatario autorizzato sia in grado di leggere e comprendere il contenuto del messaggio

Un metodo per garantire la **Segretezza** di un messaggio è attraverso la Crittografia Simmetrica o la Crittografia Asimmetrica con Chiave Pubblica

---

References

ChatGPT

Gli Algoritmi di Cifratura nei quali le lettere vengono messe a corrispondenza si dividono in due tipi

- Alfabetismo Monoalfabetico: Nel quale si utilizza un solo alfabeto
- Alfabetismo Polialfabetico: Nel quale si utilizzano più alfabeti

202303242240
Status:
Tags: Sistemi Cifratura

Alfabetismo Monoalfabetico

Un Algoritmo di Cifratura ad **Alfabetismo Monoalfabetico** utilizza un solo alfabeto per criptare i dati.
Un esempio di Algoritmo di Cifratura ad **Alfabetismo Monoalfabetico** è la Sostituzione Monoalfabetica, dove ogni lettera dell'alfabeto originale viene sostituito con un'altra lettera o simbolo.
Ad esempio, si sostituisce ogni lettera "A" con la lettera "X" e ogni lettera "B" con la lettera "Y".

Questo tipo di Crittografia è considerabile facile da decifrare, dato che viene utilizzata una mappature univoca.

References

ChatGPT

202303242245
Status:
Tags:Crittografia

Alfabetismo Polialfabetico

Un Algoritmo di Cifratura ad **Alfabetismo Polialfabetico** utilizza più alfabeti di sostituzione per criptare i dati.

References

ChatGPT

Gli Algoritmi di Cifratura vengono anche identificati in base alla regola con la quale i caratteri vengono cifrati:

- Trasposizione: Relazione tra chiave di crittografia e testo cifrato più complessa possibile
- Sostituzione: Distribuzione delle informazioni sulla chiave in tutto il testo cifrato

202303242252
Status:
Tags:

Trasposizione

Nella Crittografia, la **Trasposizione** si riferisce agli Algoritmi di Crittografia che operano sulla posizione dei caratteri del dato senza modificarne il valore.
In altre parole, questi Algoritmi riorientano l'ordine dei caratteri del testo in chiaro.

Questi sono tuttavia considerabili più deboli del metodo della Sostituzione, dato che l'ordine dei caratteri del testo in chiaro è spesso prevedibile.

È importante tenere conto che nella Matematica la **Trasposizione** si riferisce ad una Permutazione specifica nella quale solo due elementi dell'insieme vengono scambiati di posizione.

Ad **esempio**: Prendendo in considerazione l'Insieme $I = \{1, 2, 3\}$

- La **Trasposizione** di $(1, 2)$ porta al risultato $\{2, 1, 3\}$
- La **Trasposizione** di $(3, 1)$ porta al risultato $\{3, 2, 1\}$

References

ChatGPT

202303242256
Status:
Tags:Sostituzione

Sostituzione

In Crittografia, con **Sostituzione** si intendono gli Algoritmi che operano sulla sostituzione dei caratteri in chiaro con altri caratteri o simboli.
In pratica, questi Algoritmi sostituiscono ogni carattere del testo in chiaro con un carattere o simbolo corrispondente alla Chiave di Cifratura.

Questi sono considerabili più resistenti rispoetto al metodo della Trasposizione, dato che questi cambiano i valori dei caratteri del testo in chiaro e rendono più difficile l'individuazione dei modelli di frequenza dei caratteri del testo cifrato.

References

ChatGPT

Gli Algoritmi di Cifratura si identificano in base al numero di chiavi utilizzate

- Crittografia Simmetrica
- Crittografia Asimmetrica

202303242311
Status:
Tags: Sistemi Crittografia

Crittografia Simmetrica

La **Crittografia Simmetrica** utilizza una singola Chiave di Cifratura segreta condivisa tra il mittente e il destinatario per criptare e decriptare i dati.
Il problema di questo metodo è che la Chiave di Cifratura segreta deve essere condivisa in modo sicuro.

Per permettere uno scambio sicuro della singola Chiave di Cifratura si utilizza l'algoritmo dello Scambio di chiavi di Diffie-Hellman

Un esempio di Algoritmo di **Crittografia Simmetrica** è il Data Encryption Standard

---

References

202303242354
Status:
Tags:Crittografia

Scambio di chiavi di Diffie-Hellman

L'Algoritmo dello **Scambio di chiavi di Diffie-Hellman** permette lo scambio tra due parti di una Chiavi di Cifratura attraverso una comunicazione non protetta.

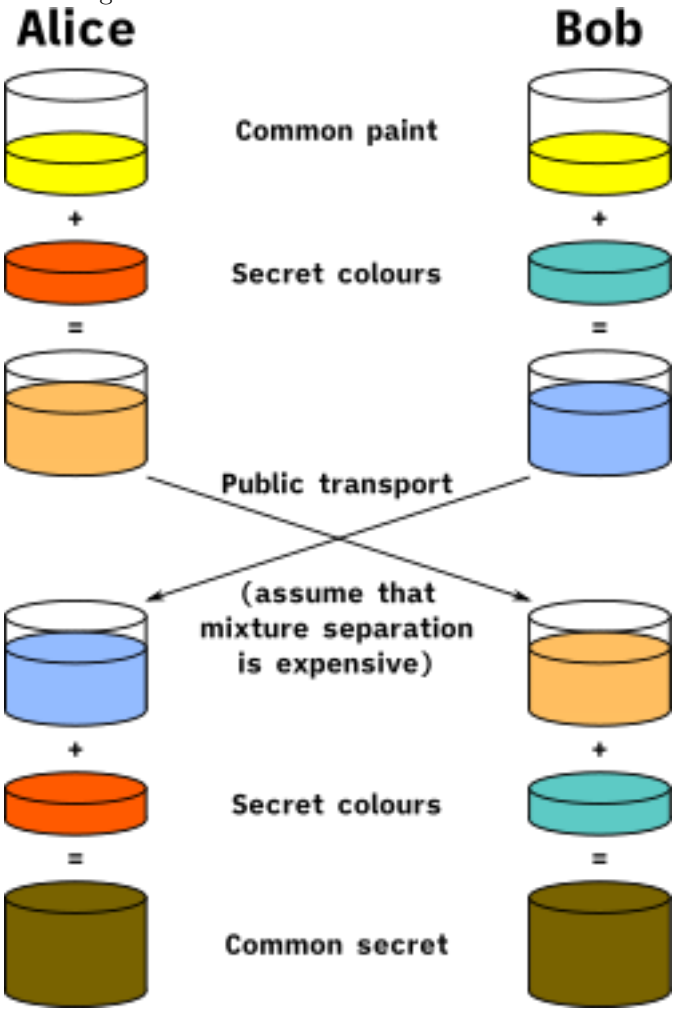
Viene generalmente utilizzato per lo scambio di Chiavi di Cifratura per Algoritmi di Crittografia Simmetrica.

Funziona quanto segue:
Alice	Bob
Possiede le chiavi pubbliche P, G	Possiede le chiavi pubbliche P, G
Sceglie il valore della chiave privata a	Sceglie il valore della chiave privata b

| Genera la chiave x
$x = G^a * mod(P)$ | Genera la chiave y
$y = G^b * mod(P)$ |
| Manda la chiave x a Bob | Manda la chiave y ad Alice |
| Riceve la chiave y da Bob | Riceve la chiave x da Alice |
| Genera la chiave segreta k_a
$k_a = y^a * mod(P)$ | Genera la chiave segreta k_b
$k_y = x^b * mod(P)$ |

Dato che algebricamente $k_a = k_b$ le due parti Alice e Bob hanno ora due chiavi simmetriche uguali.

L'Algoritmo può anche venire spiegato attraverso l'esempio dello scambio dei colori seguente:



References

Gli Algoritmi di Cifratura che utilizzano una o più chiavi seguono il Teorema di Kerckhoff, cioè che la sicurezza di un algoritmo è dato dalla chiave, non dall'algoritmo

202303270927
Status:
Tags: Sistemi

Teorema di Kerckhoff

Il **teorema di Kerchoff** è un principio fondamentale della Crittografia moderna che afferma che la sicurezza di un Cifrante non deve basarsi sulla segretezza dell'Algoritmo di Cifratura, ma piuttosto sulla Chiave di Cifratura.

Così facendo è possibile rendere l'Algoritmo pubblico per studiare la sua sicurezza più a fondo e nel caso la Chiave di Cifratura venga violata, non è necessario realizzare un nuovo Algoritmo, ma basta semplicemente cambiare Chiave di Cifratura.

References

Altri principi di Crittografia sono:

- Confusione
- Diffusione

202303270932
Status:
Tags: Sistemi

Confusione

Nella Crittografia, la **Confusione** si riferisce alla capacità di rendere la relazione tra la Chiave di Cifratura e il testo in chiaro il più complessa possibile, in modo che sia difficile dedurre la chiave a partire dal testo cifrato.

References

ChatGPT

202303270934
Status:
Tags:Sistemi

Diffusione

Nella Crittografia, la **Diffusione** si riferisce alla capacità di distribuire le informazioni sulla chiave in tutto il testo cifrato, in modo che una piccola modifica nella chiave produca una grande variazione nel testo cifrato

---

References

ChatGPT

Esempi Un esempio di Algoritmo di Cifratura utilizzato durano il IX Secolo è il Cifrario a Campale Germanico, utilizzato dalle forze armate Tedesche durante la Prima Guerra Mondiale.

Cifrario a Campale Germanico

Un'altro esempio di Algoritmo di Cifratura è quello utilizzato dalla macchina Enigma, utilizzato dalle forze armate Tedesche durante la Seconda Guerra Mondiale

202303270836
Status:
Tags:Sistemi Crittografia

Enigma

Enigma è un dispositivo Cifrante Elettromeccanico utilizzato dalle forze armate Tedesche durante la Seconda Guerra Mondiale per Cifrare e Decifrare messaggi.

I componenti della macchina sono:

- Una tastiera composta dalle 26 lettere dell'alfabeto utilizzato per inserire le lettere.

- Una ”lamp board”, composta da una serie di lampadine disposte in una griglia corrispondente alla tastiera della macchina e utilizzato per visualizzare ciascun carattere decifrato per ciascun carattere immessi dalla tastiera.
- Dei rotori che girando progressivamente ad ogni input da tastiera cifra o decifra il carattere immesso da tastiera.
- Una plugboard(o pannello di controllo), composta da una piastra con prese per cavi, dove i cavi possono essere inseriti nelle prese per scambiare le coppie di lettere.
- Una batteria interna per alimentare la macchina, rendendola così portabile

La chiave di cifratura della macchina **Enigma** è composta da:

- L'ordine della posizione dei rotori
- Ring settings, cioè la rotazione iniziale di ogni rotore.
- Configurazione della plugboard, cioè dei cavi che scambiano le coppie di lettere.

Il componente fondamentale della macchina **Enigma** sono i rotori, cioè dischi metallici sottili con 26 contatti elettrici corrispondenti alle 26 lettere dell'alfabeto latino su ambo i lati.
I rotori vengono posizionati uno accanto all'altro con i contatti uniti, in modo che il segnale passasse attraverso i contatti di tutti i rotori per poi tornare indietro.
Ad ogni carattere immesso da tastiera, il primo rotore avanza di una posizione e quando completa il giro fa avanzare il rotore successivo.
In questo modo i contatti elettrici e il carattere che ne risulta cambia ad ogni immissione da tastiera.

References

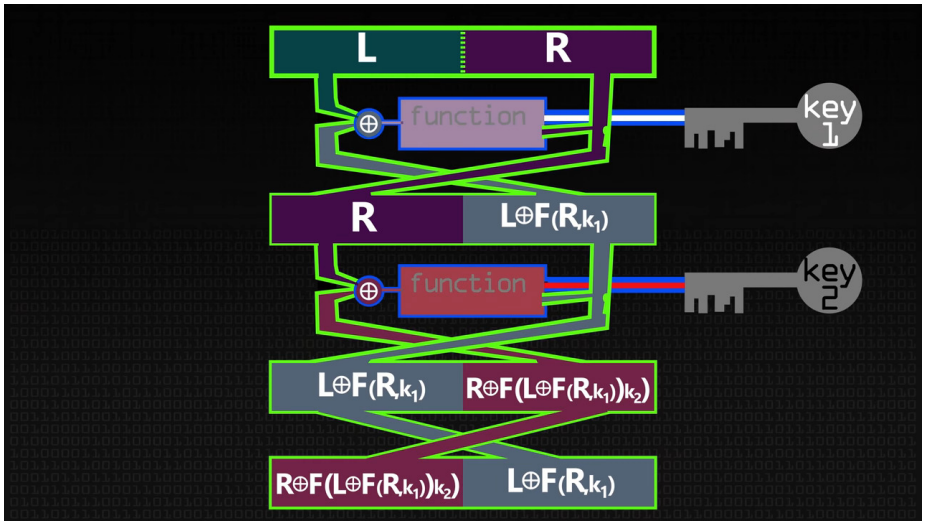
Youtube -> How did the Enigma Machine work?

202303251429
Status:
Tags: Sistemi Cifratura

Cifrario di Feistel

Il **Cifrario di Feistel** è un Algoritmo di Cifratura A Blocchi che ha preso il nome di Rete di Feistel.
Moltissimi algoritmi di Cifratura a Blocchi la utilizzato, incluso il famoso Data Encryption Standard(DES).

1. L'algoritmo divide il dato in due parti (uguali o non), la parte destra prende il nome di L e la parte sinistra prende il nome di R.
2. Primo passaggio
   (a) Al blocco posto a sinistra (cioè L) viene effettuata una funzione di Cifratura in base all'Algoritmo utilizzato, viene effettuato uno XOR($\oplus$) ,con il blocco posto a destra (cioè R) e infine spostato a destra. Matematicamente viene denoto come $L \oplus f(R, k_1)$ dove k_1 equivale alla chiave numero 1
   (b) Il blocco a destra (cioè R) viene spostato a sinistra
3. Secondo passaggio
   (a) Al blocco posto a sinistra (cioè R) viene effettuata una funzione di Cifratura in base all'Algoritmo utilizzato, viene effettuato uno XOR($\oplus$) ,con il blocco posto a destra (cioè $\oplus f(R, k_1)$) e infine spostato a destra. Matematicamente viene denoto come $R \oplus f(L \oplus f(R, k_1), k_2]$ dove k_1 equivale alla chiave numero 2
   (b) Il blocco a destra (cioè $\oplus f(R, k_1)$) viene spostato a sinistra
4. Terzo passaggio: I due blocchi vengono scambiati di posto
   (a) Il blocco a sinistra (cioè $L \oplus f(R, k_1)$) viene posto a destra
   (b) Il blocco a destra (cioè $R \oplus f(L \oplus f(R, k_1), k_2]$) viene spostato a sinistra



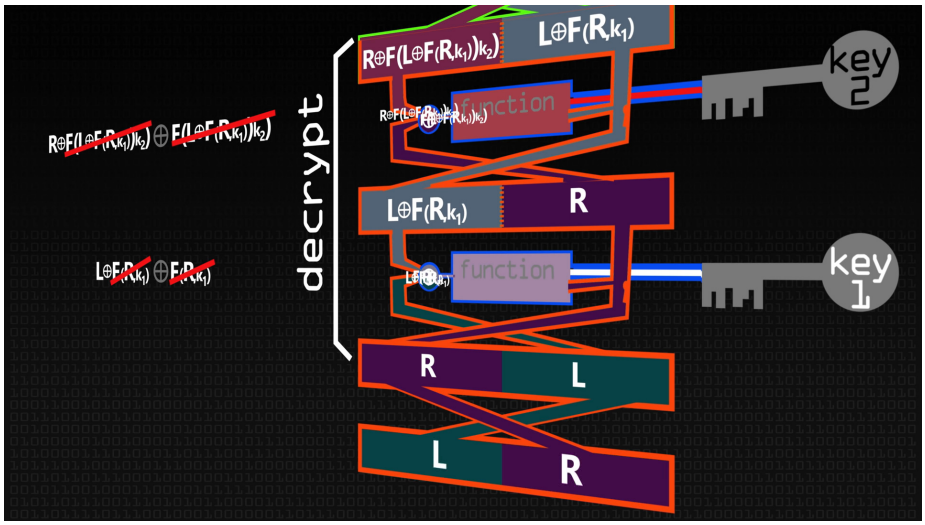
Per compiere la decifratura:

1. L'algoritmo divide il dato in due parti (uguali o non), la parte destra prende il nome di L e la parte sinistra prende il nome di R.
2. Primo passaggio
   (a) Al blocco posto a sinistra (cioè $R \oplus f(L \oplus f(R, k_1), k_2)$) viene effettuata una funzione di Cifratura in base all'Algoritmo utilizzato, viene effettuato uno XOR($\oplus$) ,con il blocco posto a destra (cioè $L \oplus f(R, k_1)$) e infine spostato a destra. Matematicamente viene de-

noto a seguito di Semplificazione come $L \oplus F(R, k_1)$ dove k_1 equivale alla chiave numero 1

   (b) Il blocco a destra (cioè $L \oplus F(R, k_1)$) viene spostato a sinistra

3. Secondo passaggio
   (a) Al blocco posto a sinistra (cioè $L \oplus F(L \oplus f(R, k_1))$) viene effettuata una funzione di Cifratura in base all'Algoritmo utilizzato, viene effettuato uno XOR($\oplus$) ,con il blocco posto a destra (cioè R) e infine spostato a destra. Matematicamente viene denoto a seguito di Semplificazione come L dove k_1 equivale alla chiave numero 2
   (b) Il blocco a destra (cioè R) viene spostato a sinistra
4. Terzo passaggio: I due blocchi vengono scambiati di posto
   (a) Il blocco a sinistra (cioè R) viene posto a destra
   (b) Il blocco a destra (cioè L) viene spostato a sinistra



References

202303250021
Status:
Tags: Sistemi

Data Encryption Standard

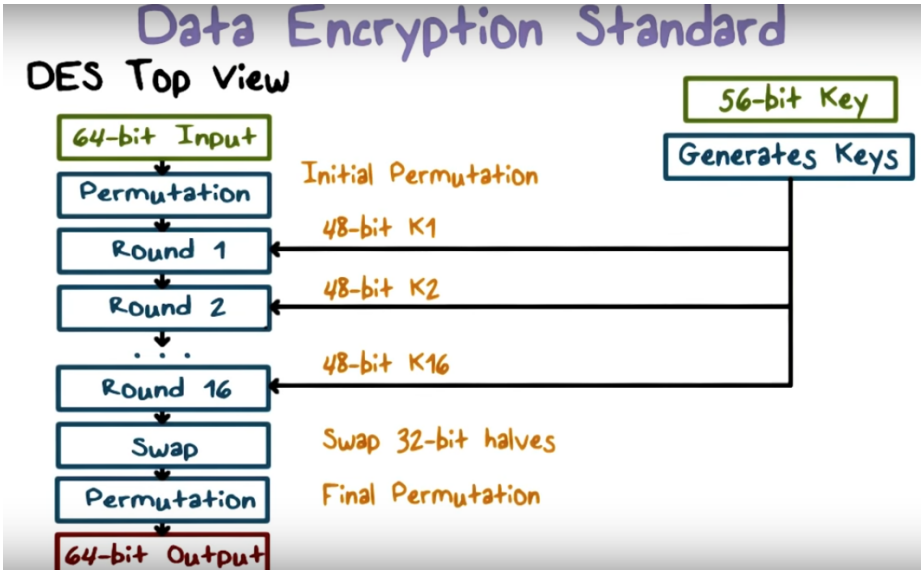
Il Data Encryption Standard è un Algoritmo di Cifratura pubblicato nel 1977 e standardizzato nel 1977.

La chiave è formata da 64 bit ed è divisa in

- 56 bit di chiave effettiva
- 8 bit di parità (ogni ottavo bit della chiave è un bit di parità)

L'Algoritmo prevede 16 round di Trasposizioni successive.
Non lavora su un alfabeto di 26 caratteri ma su file binari con byte codificati in ASCII, quindi 128 caratteri, dei quali solo 96 sono definiti stampabili (non sono caratteri speciali)

1. Il testo di 64 bit viene suddiviso in blocchi di 8 byte e codificato in ASCII per ottenere una Stringa di 64 cifre binarie
2. Avviene una Permutazione iniziale IP dei 64 bit
3. Si compiono 16 round dell'Algoritmo di Cifratura "Cifrario di Feistel".
4. Avviene una Permutazione finale inversa a quella iniziale, cioè $FP = IP^{-1}$



References

ChatGPT
Computerphile Feistel Cipher - Computerphile