Course: Crittografia

Crittografia applicata alla sicurezza di tutti i giorni: Bitwarden

Author: Edoardo Desiderio

Instructor: **Prof. Luciano Margara**

Indice

Capitolo 1

Introduzione

1.1 Scopo del Documento

L'idea della ricerca nasce poichè confrontandomi con amici e colleghi, ho notato che molti di loro studiavano il campo della crittografia da un punto di vista dei malware e dei ransomware, ma non da un punto di vista positivo. Questo documento ha lo scopo di fornire una panoramica generale della crittografia e delle sue applicazioni positive, con particolare attenzione ai password manager.

1.2 L'Uso Positivo della Crittografia

La crittografia, un campo di studio che si occupa della protezione delle informazioni attraverso l'uso di codici, ha un ruolo fondamentale nel mondo digitale di oggi. Attraverso l'utilizzo di complessi algoritmi matematici, la crittografia protegge i dati sensibili, garantisce la riservatezza delle comunicazioni, assicura l'integrità dei dati e favorisce un commercio elettronico sicuro. È uno strumento cruciale per proteggere la nostra privacy e preservare la sicurezza dei nostri dati. L'aspetto positivo di questa tecnica crittografica è la sicurezza: infatti, anche se la chiave pubblica dovesse cadere in mani "sbagliate", l'assenza della chiave privata garantisce la segretezza del messaggio. Inoltre, la crittografia è un elemento fondamentale per la cybersecurity, capace di assicurare una protezione efficace e duratura nel tempo dei sistemi e dei servizi a cui viene applicata.

Introduzione ai Password Manager

Un password manager è un sistema di sicurezza informatica, un programma che permette di creare password uniche per ogni singolo account, conservarle in un luogo sicuro e accedere ad esse attraverso un'estensione del browser o una app, sia da un computer che da un dispositivo mobile come tablet o smartphone. Questi strumenti consentono agli utenti di sincronizzare le password tra vari dispositivi, e possono o meno conservare le password e i dati anche sul dispositivo.

Storia

La storia dei password manager è intrinsecamente legata all'evoluzione della sicurezza informatica. Le password, come metodo di autenticazione, hanno radici antiche, risalenti all'antica Grecia e utilizzate per proteggere segreti militari durante la Seconda Guerra Mondiale. Con l'avvento dei computer negli anni '60, le password hanno iniziato a diventare parte della vita quotidiana.

Il primo password manager della storia è stato sviluppato nel 1990 da Mark Thompson [3] e si chiama "password Safe" e fu introdotto come software utility per windows 95.

1.3 Passwword Save e l'algoritmo di Blowfish

Password Safe, nella sua versione originale, utilizzava l'algoritmo di crittografia **Blowfish** per proteggere le password memorizzate. Blowfish è un algoritmo di crittografia a blocchi simmetrico sviluppato da Bruce Schneier nel 1993.

- **Crittografia Simmetrica:** Usa la stessa chiave per crittografare e decrittografare i dati.
- **Lunghezza della Chiave Variabile:** Supporta chiavi di lunghezza variabile, da 32 a 448 bit, rendendolo flessibile in base alle esigenze di sicurezza.
- **Dimensione del Blocco:** Opera su blocchi di dati di 64 bit.
- **S-Box:** Utilizza strutture interne note come S-box per realizzare la crittografia.

1.4 Funzionamento di Blowfish

Blowfish utilizza un insieme di operazioni come sostituzioni e permutazioni, gestite attraverso S-box e , per trasformare il testo in chiaro in testo cifrato. Ogni blocco di dati viene elaborato in 16 round di crittografia.

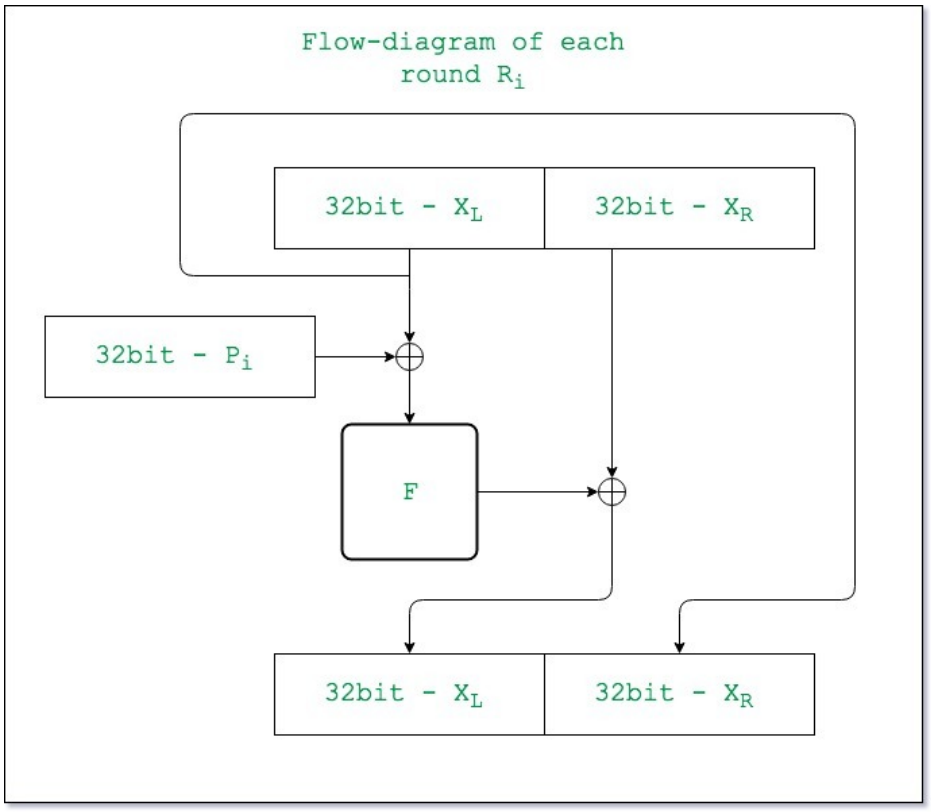

Figura 1.1: grafico che cattura il processo di crittografia dell'algoritmo [1]

Processo di Crittografia e Decrittografia

il processo principale di crittografia e decrittografia di Blowfish sta tutto nella funzione `f` che utilizza le S-box per creare una funzione non lineare che contribuisce alla sicurezza dell'algoritmo.

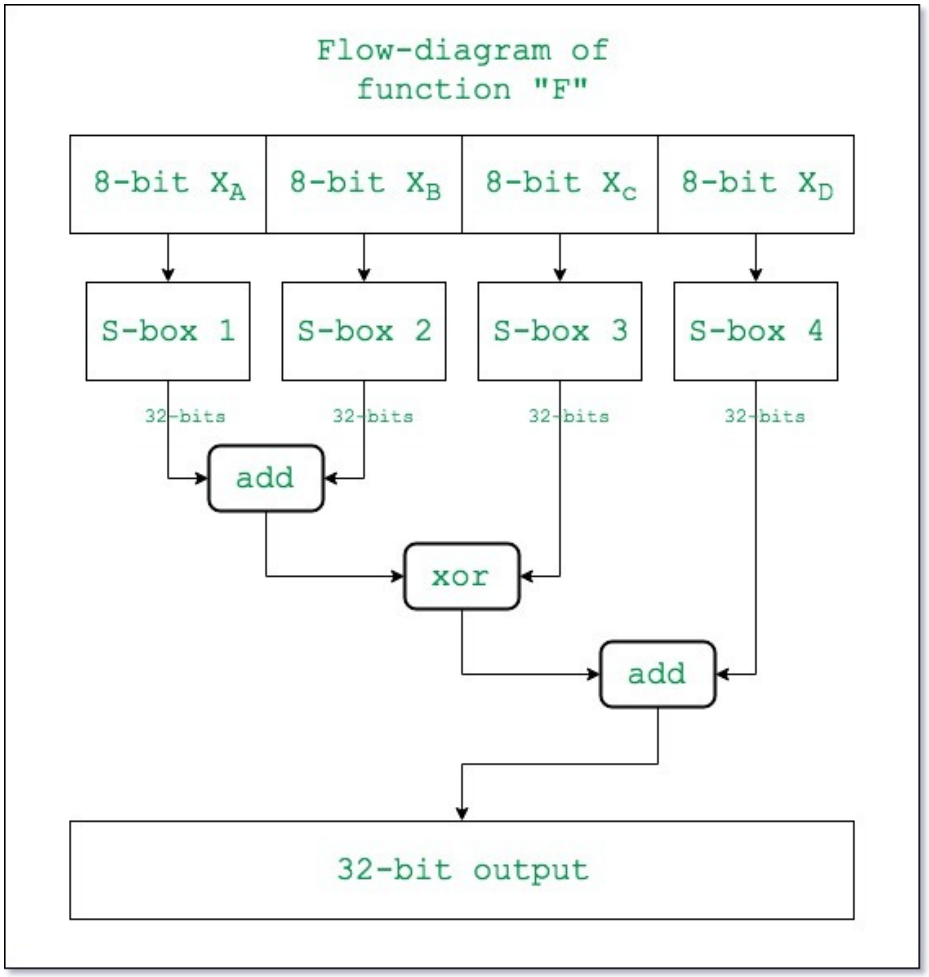

Figura 1.2: metodo f dell'algoritmo [1]

Funzione F dell'algoritmo Blowfish

La funzione F prende in input un valore di 32 bit x e restituisce un valore di 32 bit. Essa viene definita come segue:

$$F(x) = ((S_1[a] + S_2[b] \bmod 2^{32}) \oplus S_3[c]) + S_4[d] \bmod 2^{32}$$

- S_1, S_2, S_3, S_4 sono le S-box dell'algoritmo.
- a byte più significativo di x.
- b = secondo byte più significativo di x

- c = secondo byte meno significativo di x
- d = byte meno significativo di x

```
1    function F(x):
2      result = ((S1[a] + S2[b] mod 2^32) xor S3[c])
          + S4[d] mod 2^32
3
4      return result
```

conclusioni

in pratica l'algoritmo di crittografia Blowfish si differenzia principalmente dal DES visto a lezione per la sua chiave variabile fino a 448 bit. [2]

Bibliografia

[1] GeeksforGeeks contributors. Blowfish algorithm. https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/. Accessed: 2/07/2024 15:00.

[2] GeeksforGeeks contributors. Blowfish algorithm. https://www.baeldung.com/cs/des-vs-3des-vs-blowfish-vs-aes, note = Accessed: 2/07/2024 15:30.

[3] Wikipedia contributors. Password manager. https://en.wikipedia.org/wiki/Password_manager. Accessed: 2/07/2024 12:00.

Riferimenti bibliografici