University of Pisa

Department of Information Engineering

Foundation Of Cybersecurity

Nicolò Mariano Fragale

March 2025

Contents

Information

These notes are intended for educational purposes only and cover essential concepts in the field of data systems and security. The aim is to provide a comprehensive understanding of topics such as system vulnerabilities, protection techniques, and defense strategies in cybersecurity.

This document includes topics related to access control, authentication mechanisms, database security, cryptographic methods, and advanced persistent threats, with a particular focus on practical applications in real-world scenarios.

1 Symmetric cryptography

2 Asymmetric cryptography

2.1 RSA

2.2 Diffie-Hellman exchange

- **Groups:** è un insieme G dotato di un'operazione binaria $*$ che soddisfa le seguenti proprietà (modulo p omesso negli esempi):
  - **Chiusura**: Per ogni $a, b \in G$, si ha $a * b \in G$.
  - **Associatività**: Per ogni $a, b, c \in G$, vale $(a * b) * c = a * (b * c)$.
  - **Elemento neutro**: Esiste un elemento $e \in G$ tale che per ogni $a \in G$, si ha $a * e = e * a = a$.
  - **Elemento inverso**: Per ogni $a \in G$, esiste un elemento $a^{-1} \in G$ tale che $a * a^{-1} = a^{-1} * a = e$.

  Se inoltre l'operazione è **commutativa** ($a * b = b * a$ per ogni $a, b \in G$), il gruppo è detto **abeliano**.
- **Sub-Groups:** Porzione di gruppo;
- **Finite Groups:** Gruppo con numero finito di elementi;
- **Ciclic Groups:** Un gruppo ciclico è un gruppo che contiene almeno un elemento g (detto generatore) tale che tutte le potenze (o iterazioni dell'operazione del gruppo) di quel generatore generano tutti gli altri elementi del gruppo. $\rightarrow$ G = $\{g^k \mid k \in \mathbb{Z}\}$

$\mathbb{Z}_p^*$: è l'insieme degli interi da 1 a p-1, con l'operazione di moltiplicazione modulo p (escluso 0).

Il protocollo di **Diffie-Hellman Key Exchange** permette a due parti di concordare una chiave segreta condivisa su un canale insicuro. Vediamo il processo con un esempio pratico.

Parametri pubblici

Prima di tutto, Alice e Bob scelgono un numero primo pubblico p (modulo) e una base (o generatore) g:

- Numero primo pubblico: $p = 23$
- Generatore pubblico: $g = 5$

Questi valori sono conosciuti da tutti e possono essere intercettati senza problemi.

Scelta delle chiavi private

Alice e Bob scelgono ciascuno una chiave privata segreta:

- Chiave privata di Alice: $a = 6$
- Chiave privata di Bob: $b = 15$

Calcolo delle chiavi pubbliche

Entrambi calcolano le rispettive chiavi pubbliche usando la formula:

$$X = g^a \mod p$$

- Alice calcola: $A = 5^{6} \mod 23 = 8$
- Bob calcola: $B = 5^{15} \mod 23 = 19$

Ora Alice e Bob si scambiano pubblicamente A e B.

Calcolo della chiave segreta condivisa

Alice e Bob ora utilizzano il valore pubblico ricevuto per calcolare la chiave segreta condivisa:

- Alice calcola: $S = B^{a} \mod p = 19^{6} \mod 23 = 2$
- Bob calcola: $S = A^{b} \mod p = 8^{15} \mod 23 = 2$

Entrambi arrivano alla stessa chiave segreta 2, che ora può essere usata per cifrare la comunicazione!

Considerazioni sulla Sicurezza

Un attaccante che intercetta i messaggi vede solo p, g, A e B, ma per calcolare S dovrebbe risolvere il problema del logaritmo discreto, che è computazionalmente difficile se i numeri sono sufficientemente grandi. Per questo motivo è fondamentale usare un numero che sia molto grande (migliaia di bit) e primo.

Man-in-the-middle attack e solution:

Il Man-in-the-Middle (MitM) attack durante lo scambio di chiavi Diffie-Hellman (DH) è un problema serio, poiché il protocollo base non fornisce autenticazione. Un attaccante può intercettare e sostituire le chiavi pubbliche scambiate tra le due parti, instaurando due connessioni separate (una con ciascuna parte) e decrittando i messaggi.
Soluzioni:

- Sfruttare PKI (public key infrastructure) per autenticare le chiavi pubbliche firmante da un autorità certificata.
- Chiavi firmate con RSA.
- Viene autenticato e reso sicuro il canale di comunicazione

Quando si dice che Diffie-Hellman è un protocollo non interattivo, si fa riferimento al fatto che i due partecipanti (ad esempio, Alice e Bob) possono stabilire una chiave segreta condivisa senza la necessità di scambiarsi messaggi diretti in tempo reale o interagire direttamente in ogni passaggio.

2.3 DLP(Discrete Logarithm Problem) :

è un problema matematico che si basa sull'operazione di moltiplicazione in gruppi, in particolare in gruppi ciclici.
In altre parole, dato g (generatore di G) e h (appartente a G), il compito è trovare x, ovvero il logaritmo discreto, tale che elevando g alla potenza x modulo p si ottiene h.

Supponiamo di avere un gruppo $\mathbb{Z}_p^*$ (ad esempio, $p = 7$), con il generatore $g = 3$, e vogliamo trovare x tale che $3^x \equiv 4 \mod 7$. Il problema del logaritmo discreto è trovare x che soddisfi questa equazione.

1. $3^1 = 3 \mod 7$
2. $3^2 = 9 \mod 7 = 2$
3. $3^3 = 6 \mod 7$
4. $3^4 = 18 \mod 7 = 4$

Quindi, $x = 4$ è la soluzione, perché $3^4 \equiv 4 \mod 7$.

Non esiste un algoritmo efficiente (polinomiale) per risolvere il DLP in generale, rendendo la sicurezza di molti algoritmi crittografici basati su DLP molto solida.

If DLP can be easily solved, then DHP can be easily solved.
DLP can be applied for any cyclic group.
DLP id indipendent of the generator.

DLP è usato in:

- Diffie-Hellman Key Exchange
- DSA (Digital Signature Algorithm)
- ElGamal Encryption
- ECDSA (Elliptic Curve Digital Signature Algorithm)
- Lattice-based Cryptography
- Schnorr signature

In $\mathbb{Z}_p^*$, to achieve 80-bit security, the prime p must be at least 1024 bit long, it is more efficiente than $GF(2^m)$.

2.4 Galois Field $GF(2^m)$ è un campo finito che contiene 2^m elementi.

Come esempio pratico, m = 256 è una dimensione comunemente utilizzata per garantire un livello di sicurezza simile a 2048 bit in un gruppo basato su $\mathbb{Z}_p^*$.

Sebbene si possa definire un DLP in un campo finito come $GF(2^m)$, non è ideale come base per la crittografia. Questo perché il problema risulta relativamente più facile da risolvere rispetto al DLP in $\mathbb{Z}_p^*$. Sebbene il DLP in $GF(2^m)$ non sia ideale, le curve ellittiche su campi finiti come $GF(2^m)$ sono molto sicure e efficienti. Le curve ellittiche offrono una sicurezza elevata con chiavi più corte e sono ampiamente utilizzate in crittografia moderna, grazie alla loro resistenza a determinati attacchi e alle loro operazioni efficienti.

In sintesi:

- Per il DLP, $\mathbb{Z}_p^*$ è la scelta migliore.

- Per la sicurezza avanzata e l'efficienza, le curve ellittiche su $GF(2^m)$ sono preferite, ma non sono utilizzate per il DLP tradizionale.

2.5 DLP in cyclic subgroup Usare il DLP in un sottogruppo ciclico di ordine primo grande è più sicuro, più efficiente e resistente agli attacchi.
Sottogruppo: Un sottogruppo è semplicemente una parte di un gruppo che segue le stesse regole del gruppo originale.
Il teorema di Lagrange dice che l'ordine di un sottogruppo deve essere un divisore dell'ordine del gruppo. */rightarrow* Se G ha ordine 12, i possibili sottogruppi avranno ordini 1, 2, 3, 4, 6, 12 (tutti i divisori di 12).
Se G è ciclico, ogni sottogruppo è anch'esso ciclico ed ha esattamente un sottogruppo per ogni divisore di n. */rightarrow* Se G ha ordine 12 allora esistono esattamente 6 sottogruppi per ogni divisore.

N.B! DH si applica tipicamente a un sottogruppo ciclico di ordine primo (che ha come ordine (ordine: cardinalità del gruppo) un numero primo) grande (se g cade in un sottogruppo piccolo allora il DLP diventa facile da risolvere).
Come si sceglie un sottogruppo ciclico di ordine primo grande?

- Scegliere un numero primo p grande (2048 bit) tale che $p = 2q + 1$ con q primo.
- Scegliere un generatore g che appartiene a q
- Si verifica che
$$g^q \equiv 1 \mod p$$
, assicurandosi che g appartenga davvero al sottogruppo di ordine q.