

Introduzione alla Crittografia e Principi Fondamentali

1. 📖 Spiegazione Approfondita

La crittografia non è semplicemente una tecnica di occultamento, ma una disciplina scientifica fondamentale per la sicurezza informatica moderna. Il suo scopo primario è trasformare informazioni leggibili (plaintext) in una forma illeggibile (ciphertext) per proteggerle da accessi non autorizzati. In un'era dominata dalla comunicazione digitale, la crittografia è il pilastro che garantisce la protezione dei dati sensibili, la privacy personale e aziendale, e la sicurezza delle transazioni finanziarie.

Lo studio di questa materia è vitale per quattro ragioni principali delineate nel corso:

1. **Protezione dei dati sensibili:** Salvaguardia di informazioni critiche (es. dati bancari, sanitari) da occhi indiscreti.
2. **Sicurezza delle comunicazioni:** Garanzia che i canali di trasmissione (email, messaggistica, web) siano protetti da intercettazioni.
3. **Autenticazione e integrità:** Verifica dell'identità delle parti comunicanti e assicurazione che i dati non siano stati manipolati.
4. **Privacy e anonimato:** Tutela dell'identità digitale dell'utente.

I **quattro pilastri (o obiettivi)** della crittografia moderna sono:

- **Riservatezza (Confidentiality):** Garantisce che l'informazione sia accessibile *solo* a chi è esplicitamente autorizzato. La cifratura impedisce la lettura dei dati a terzi non autorizzati.
- **Integrità (Integrity):** Assicura che i dati non abbiano subito alterazioni non autorizzate durante la trasmissione o lo stoccaggio. Si ottiene tramite meccanismi come le funzioni di *hash*.
- **Autenticazione (Authentication):** Conferma l'identità dei soggetti coinvolti (chi invia e chi riceve). Si avvale di certificati digitali e protocolli specifici.
- **Non ripudio (Non-repudiation):** Impedisce a un soggetto di negare la paternità di un'azione o l'invio di un messaggio. La prova crittografica (spesso la firma digitale) lega indissolubilmente l'autore al messaggio.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** La crittografia è la scienza che trasforma il *plaintext* in *ciphertext* tramite algoritmi matematici e chiavi, garantendo confidenzialità, integrità, autenticazione e non ripudio.
- **Contesto Reale:** In azienda, questi principi si applicano ovunque: la *riservatezza* protegge i segreti industriali, l'*integrità* assicura che i bonifici non vengano modificati nell'importo, l'*autenticazione* permette l'accesso alle VPN, e il *non ripudio* ha valore legale nei contratti firmati digitalmente.

5. ⚠️ Focus Esame

- **Domanda frequente:** Qual è la differenza tra Integrità e Autenticazione? L'integrità riguarda il *dato* (non è cambiato), l'autenticazione riguarda il *soggetto* (è chi dice di essere).
- **Trabocchetto:** Confondere il "Non ripudio" con l'anonimato. Sono opposti: il non ripudio serve proprio a provare legalmente chi ha fatto cosa.

Terminologia Essenziale: Plaintext, Cifrario e Chiavi

1. 📖 Spiegazione Approfondita

Per operare in ambito crittografico è necessario padroneggiare il vocabolario tecnico di base:

- **Plaintext (Testo in chiaro):** Sono i dati originali, leggibili e comprensibili (es. "Ciao mondo", un numero di carta di credito). È l'input del processo di cifratura.
- **Cifrario (Cipher):** È l'algoritmo matematico (la logica o la "ricetta") utilizzato per trasformare il plaintext in ciphertext e viceversa. Esempi noti includono AES (simmetrico) e RSA (asimmetrico).
- **Chiave di Crittografia:** È il valore segreto (una stringa di bit) che parametrizza il cifrario. Senza la chiave, l'algoritmo da solo non garantisce sicurezza (principio di Kerckhoffs: la sicurezza risiede nella chiave, non nell'algoritmo).
- **Crittotesto (Ciphertext):** L'output del processo di cifratura. Appare come una sequenza pseudo-casuale di caratteri incomprensibili.

Le chiavi si dividono in due grandi famiglie:

1. **Chiavi Simmetriche:** Una sola chiave condivisa per cifrare e decifrare. Veloce, ma problematica nella distribuzione (come faccio a darti la chiave senza che qualcuno la intercetti?).
2. **Chiavi Asimmetriche:** Una coppia di chiavi. Una *Pubblica* (per cifrare) e una *Privata* (per decifrare). Risolve il problema della distribuzione ma è computazionalmente più lenta.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Il *Cifrario* è il motore logico, la *Chiave* è il carburante unico. Senza la chiave corretta, il motore non può invertire il processo (decifratura).
- **Contesto Reale:** Quando configuri il Wi-Fi di casa (WPA2), la password che inserisci è la base per generare la *Chiave Simmetrica* che protegge il traffico.

Cifrario di Cesare (Crittografia Storica)

1. 📖 Spiegazione Approfondita

Il Cifrario di Cesare è l'esempio canonico di crittografia a sostituzione monoalfabetica. Utilizzato da Giulio Cesare per le comunicazioni militari, si basa su un principio elementare: lo scorrimento (shift) dell'alfabeto.

- **Meccanismo:** Ogni lettera del messaggio in chiaro viene sostituita dalla lettera che si trova un numero fisso di posizioni più avanti nell'alfabeto.
- **La Chiave:** Il numero di posizioni dello spostamento (nello storico "shift di 3").
- **Modularità:** Se si raggiunge la fine dell'alfabeto (Z), si ricomincia dalla A (aritmetica modulare).

Esempio (Shift 3):

- Plaintext: **A** -> Ciphertext: **D**
- Plaintext: **B** -> Ciphertext: **E**
- Plaintext: **T** -> Ciphertext: **W**
- Plaintext: **ATTACCARE** -> Ciphertext: **DWWDFFDUH**

4. 🔗 Cross-Connection Master

- **Integrazione Extra-Slide (Coding/Python):** Implementare il cifrario di Cesare è un classico esercizio di programmazione. Si utilizza il valore ASCII dei caratteri: `char_cifrato = (char_originale + key) % 26`.

5. ⚠ Focus Esame

- **Criticità:** Il Cifrario di Cesare è **estremamente insicuro** oggi. Può essere rotto istantaneamente con un attacco di "Brute Force" (provando i soli 25 spostamenti possibili) o con l'analisi delle frequenze (es. la lettera 'E' è la più comune in molte lingue, quindi nel testo cifrato il simbolo più frequente sarà probabilmente la 'E' cifrata).

Crittografia Simmetrica

1. 📖 Spiegazione Approfondita

La crittografia simmetrica (o a chiave privata/segreta) è la tecnica in cui mittente e destinatario condividono **la stessa identica chiave** per le operazioni di cifratura e decifratura.

Processo:

1. Mittente cifra il Plaintext con la Chiave K -> Crittotesto.
2. Destinatario usa la Chiave K sul Crittotesto -> Plaintext.

Algoritmi Comuni (Analisi Slide):

- **AES (Advanced Encryption Standard):** Lo standard globale attuale. Cifrario a blocchi, sicuro ed efficiente. Supporta chiavi a 128, 192 e 256 bit.
- **DES (Data Encryption Standard):** Obsoleto. Usava chiavi a 56 bit, oggi facilmente violabili con la forza bruta.
- **3DES (Triple DES):** Evoluzione del DES che applica l'algoritmo tre volte per aumentare la sicurezza, ma è lento e in dismissione.
- **RC4:** Cifrario a flusso (stream cipher). Famoso per la velocità ma noto per gravi vulnerabilità (usato nel vecchio protocollo WEP del Wi-Fi, ora insicuro).

Pro e Contro:

- **Vantaggi:** Efficienza (molto veloce), basso consumo di risorse CPU. Adatto per cifrare grandi moli di dati (es. interi hard disk).
- **Svantaggi: Gestione delle chiavi (Key Distribution Problem).** Come condividere la chiave in modo sicuro? Inoltre, scarsa scalabilità: in una rete di 100 persone, servirebbero migliaia di chiavi per far parlare tutti con tutti in modo privato.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** *Simmetrica* significa "speculare": la stessa chiave chiude e apre.
- **Contesto Reale:** AES-256 è utilizzato per criptare i database aziendali a riposo (Data at Rest) e per la parte "veloce" delle connessioni VPN.

Crittografia Asimmetrica (A Chiave Pubblica)

1. 📖 Spiegazione Approfondita

La crittografia asimmetrica risolve il problema dello scambio delle chiavi introducendo una coppia di chiavi matematicamente correlate ma distinte:

1. **Chiave Pubblica:** Distribuibile liberamente a chiunque. Usata per **cifrare** i messaggi destinati al proprietario o per **verificare** le firme.
2. **Chiave Privata:** Custodita gelosamente dal proprietario. Usata per **decifrare** i messaggi ricevuti o per **firmare** documenti.

Flusso di Riservatezza (Esempio Alice -> Bob):

- Alice vuole scrivere a Bob.
- Alice recupera la **Chiave Pubblica di Bob**.
- Alice cifra il messaggio con la Chiave Pubblica di Bob.
- Solo Bob (che possiede la **Chiave Privata di Bob**) può decifrare il messaggio.

Algoritmi Comuni:

- **RSA (Rivest-Shamir-Adleman):** Basato sulla fattorizzazione di grandi numeri primi. Chiavi lunghe (2048/4096 bit).
- **ECC (Elliptic Curve Cryptography):** Basato sulle curve ellittiche. Offre pari sicurezza di RSA ma con chiavi molto più corte (es. 256 bit ECC \approx 3072 bit RSA), risultando più efficiente per dispositivi mobili.
- **DSA (Digital Signature Algorithm):** Specifico per le firme digitali.

Pro e Contro:

- **Vantaggi:** Risolve il problema della distribuzione delle chiavi (la pubblica può viaggiare in chiaro); Garantisce autenticazione e non ripudio.
- **Svantaggi:** Lentezza computazionale (ordini di grandezza più lento della simmetrica); le chiavi sono più lunghe (occupano più memoria).

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** "Cifro con la pubblica del destinatario, il destinatario decifra con la sua privata".
- **Contesto Reale:** Quando ti connetti a un sito HTTPS, la crittografia asimmetrica viene usata *solo all'inizio* per scambiare in sicurezza la chiave simmetrica, che verrà poi usata per la velocità (crittografia ibrida).

5. ⚠️ Focus Esame

- **Trabocchetto Classico:** "Se cifro con la mia chiave privata, sto garantendo la segretezza?" **NO**. Se cifri con la tua privata, *chiunque* abbia la tua pubblica può decifrare. Questa operazione serve per la *Firma Digitale* (autenticità), non per la segretezza.

Firma Digitale

1. 📖 Spiegazione Approfondita

La firma digitale è l'equivalente elettronico, ma crittograficamente superiore, della firma autografa. Garantisce tre proprietà critiche: **Integrità, Autenticità, Non Ripudio**.

Il Processo Tecnico (Step-by-Step):

1. **Hashing:** Il mittente crea un "impronta digitale" (Hash) del documento originale. L'hash è una stringa di lunghezza fissa che rappresenta univocamente il file.
2. **Cifratura dell'Hash (Firma):** Il mittente cifra *solo l'hash* utilizzando la propria **Chiave Privata**. Il risultato è la Firma Digitale.
3. **Invio:** Il mittente spedisce il documento (in chiaro o cifrato, non importa ai fini della firma) + la Firma Digitale.
4. **Verifica (Destinatario):**
 - Il destinatario calcola autonomamente l'hash del documento ricevuto.
 - Il destinatario decifra la Firma Digitale usando la **Chiave Pubblica** del mittente, ottenendo l'hash originale.
 - **Confronto:** Se l'hash calcolato e l'hash decifrato coincidono, la firma è valida.

Perché è sicura?

- Se il documento cambia anche di un solo bit, l'hash cambia -> Verifica fallita (Integrità).
- Solo il possessore della chiave privata poteva cifrare quell'hash -> Identità confermata (Autenticità/Non Ripudio).

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** La firma digitale è un hash cifrato con la chiave privata del mittente.
- **Contesto Reale:** Fatturazione elettronica, firma di contratti PDF, aggiornamenti software (Windows verifica che l'update sia firmato da Microsoft).

Certificati Digitali e CA (Certification Authority)

1. 📖 Spiegazione Approfondita

Come faccio a fidarmi che la Chiave Pubblica che trovo online sia davvero di "Bob" e non di un attaccante? Qui entrano in gioco i Certificati Digitali.

Il Certificato Digitale: È un "passaporto elettronico" che lega un'identità (Soggetto) a una Chiave Pubblica, firmato da un ente fidato. Segue lo standard **X.509**.

Struttura X.509 (Campi principali):

- **Versione & Numero di Serie:** Identificativi univoci.
- **Algoritmo di Firma:** Es. SHA-256 con RSA.
- **Emittente (Issuer):** Chi ha rilasciato il certificato (la CA).
- **Validità:** Data inizio e fine (scadenza).
- **Soggetto (Subject):** Chi è il proprietario (es. www.google.com o Mario Rossi).
- **Chiave Pubblica del Soggetto:** Il payload più importante.
- **Firma della CA:** La garanzia di autenticità.

Certification Authority (CA): La CA è la terza parte fidata (Trusted Third Party). Il suo ruolo nella PKI (Public Key Infrastructure) è:

1. **Verifica:** Controlla l'identità di chi richiede un certificato.
2. **Emissione:** Crea il certificato e lo firma con la propria chiave privata CA.
3. **Gestione/Revoca:** Mantiene le liste dei certificati non più validi (CRL - Certificate Revocation List) o risponde a query di stato (OCSP).

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Un certificato digitale "certifica" che una specifica chiave pubblica appartiene a uno specifico soggetto. La fiducia si basa sulla firma della CA.
- **Contesto Reale:** Il lucchetto nel browser. Il browser si fida di una lista di CA preinstallate (Root CA); se il certificato del sito è firmato da una di queste, il sito è considerato sicuro.

Crittografia in Trasmissione: TLS/SSL

1. 📖 Spiegazione Approfondita

TLS (Transport Layer Security) e il suo predecessore (ormai insicuro) SSL (Secure Sockets Layer) sono protocolli che proteggono i dati in transito su rete IP.

- **SSL:** Nato nel 1995 (Netscape). Deprecato.
- **TLS:** Evoluzione standardizzata. Le versioni sicure attuali sono TLS 1.2 e 1.3.

Applicazioni: HTTPS (Web sicuro), VPN, SMTPS (Email sicura).

Il Protocollo Handshake (Come avviene la connessione sicura):

1. **Client Hello:** Il client propone versioni TLS e cifrari supportati.
2. **Server Hello:** Il server sceglie la configurazione e invia il proprio **Certificato Digitale**.
3. **Verifica:** Il client verifica la validità del certificato del server (tramite CA).
4. **Key Exchange (Scambio Chiavi):** Client e Server usano algoritmi asimmetrici (es. Diffie-Hellman o RSA) per concordare una **Chiave di Sessione Simmetrica**.
5. **Sessione Sicura:** Da questo momento in poi, tutto il traffico è cifrato con la chiave simmetrica (più veloce). Viene garantita anche l'integrità tramite MAC (Message Authentication Code).

2. ✂️ Sintassi & Comandi (Cleaning)

Le slide citano l'URL.

- Corretto: <https://www.bancaesempio.com>
- Nota: Il prefisso <https://> forza il browser a innescare l'handshake TLS sulla porta 443.

5. ⚠️ Focus Esame

- **Domanda:** Perché si usa una chiave di sessione simmetrica invece di continuare con quella asimmetrica?
- **Risposta:** Per le **prestazioni**. La crittografia asimmetrica è troppo lenta per cifrare l'intero flusso di dati (streaming, caricamento pagine). Si usa l'asimmetrica solo per scambiare la chiave veloce

(simmetrica).

Steganografia

1. 📖 Spiegazione Approfondita

La steganografia si distingue nettamente dalla crittografia per l'obiettivo finale.

- **Crittografia:** Nasconde il *contenuto* del messaggio (si vede che c'è un messaggio cifrato, ma non si capisce cosa dice).
- **Steganografia:** Nasconde l'*esistenza* stessa del messaggio. Il messaggio segreto è incorporato in un contenitore (carrier) apparentemente innocuo in modo invisibile all'occhio umano.

Tipi di Steganografia:

1. **Immagini:** Modifica dei bit meno significativi (LSB - Least Significant Bit) dei pixel per codificare informazioni. L'occhio umano non percepisce la variazione di colore minima.
2. **Audio:** Nascondere dati nelle frequenze non udibili o nei bit meno significativi dei campioni audio.
3. **Video/Testo:** Tecniche analoghe su flussi video o formattazione del testo.

3. 🧠 Analisi Tecnica & Memorizzazione

- **Definizione Chiave:** Sicurezza tramite oscurità (Security through obscurity). Mentre la crittografia è matematica, la steganografia è dissimulazione.
- **Contesto Reale:** Malware che nascondono codice malevolo dentro immagini JPEG scaricate da siti legittimi per evadere i controlli antivirus.

4. 🔗 Cross-Connection Master

- **Integrazione Pentesting:** Strumenti come **steghide** o **zsteg** sono usati nelle competizioni CTF (Capture The Flag) per estrarre flag nascoste nelle immagini. Spesso Crittografia e Steganografia vengono usate insieme: un messaggio cifrato (per sicurezza) viene poi nascosto steganograficamente (per invisibilità).