01001001 01101110 01100110 01101111

01000001 01101100 01100111 01101111

Crittografia e dintorni: decodificare la finanza con AI

01000100 01100101 01100011 01110010

Università Cattolica del Sacro Cuore
27 Ottobre 2025
Matteo Gregorini

01010100 01100101 01100011 01101110

01000011 01110010 01101001 01110000

Outline della Presentazione

1. Storia della Crittografia

- I primi cifrari
- Cifrari a sostituzione
- Cifrari Alfabetici

2. Crittografia Moderna

- La Rivoluzione di Shannon
- La Crittografia Moderna
- I meccanismi delle chiavi

3. Criptovalute ed AI

- Bitcoin: La prima criptovaluta
- Sicurezza Crittografica nelle Criptovalute
- L'impatto dell'AI sulla crittografia

A	B	C	D	E	F
A	B	C	D	E	F
B	C	D	E	F	G
C	D	E	F	G	H

01001001 01101110 01100110 01101111

01000001 01101100 01100111 01101111

01000100 01100101 01100011 01110010

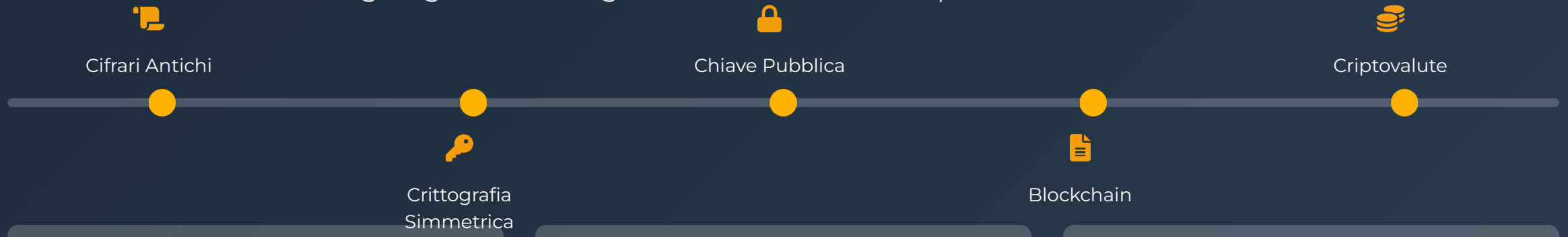
1 - Storia della Crittografia

01010100 01100101 01100011 01101110

01000011 01110010 01101001 01110000

Introduzione

Questo percorso traccia l'evoluzione scientifica e matematica della sicurezza delle informazioni, dalla semplice sostituzione dei caratteri agli algoritmi crittografici avanzati e dalle criptovalute alla blockchain.



Sicurezza

La protezione delle informazioni contro la crittoanalisi.

Blockchain

Un registro pubblico, decentralizzato e immutabile.

Intelligenza Artificiale

Strumento e sfida per la crittografia moderna.

I Primi Cifrari: Trasposizione

Cifrari a Trasposizione

I metodi di cifratura a trasposizione riorganizzano le lettere di un messaggio senza modificarle.

La Scitala Greca

- Strumento usato dagli antichi Greci per comunicazioni segrete
- Consisteva in una striscia di pergamena avvolta attorno a un cilindro di diametro specifico
- Il messaggio veniva scritto lungo la lunghezza della striscia
- Srotolata, le lettere apparivano mescolate
- Poteva essere letta correttamente solo riavvolgendo la striscia attorno a un cilindro di diametro identico

Quando la striscia è srotolata, le lettere appaiono mescolate e illeggibili.

Solo con il cilindro giusto si può leggere il messaggio originale.

Cifrari a Sostituzione

Cifrario di Cesare

Metodo di sostituzione monoalfabetica in cui ogni lettera viene spostata di un certo numero di posizioni nell'alfabeto.

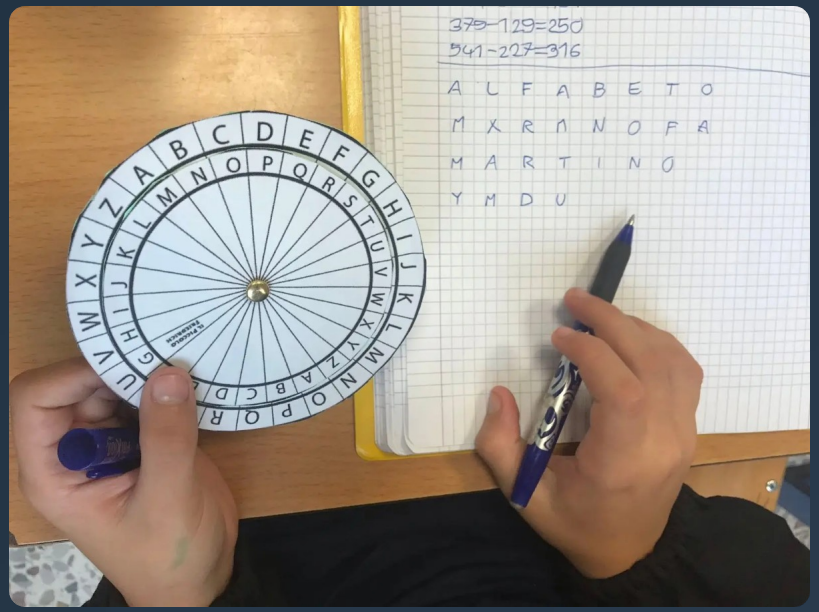
$$C \equiv (P + k) \bmod 26$$

- C: lettera cifrata
- P: lettera in chiaro
- k: chiave (spostamento)

26: numero di lettere nell'alfabeto

Vulnerabilità

Altamente vulnerabile all'analisi di frequenza, che sfrutta la distribuzione non uniforme delle lettere in una lingua.



Funzionamento

Ogni lettera del messaggio in chiaro viene sostituita con una lettera che si trova k posizioni più avanti nell'alfabeto. Se si supera la Z, si ricomincia da A.

Evoluzione dei Cifrari: Polialfabetici

Cifrari Polialfabetici

I cifrari polialfabetici furono sviluppati per contrastare l'analisi di frequenza, che poteva decifrare i cifrari a sostituzione monoalfabetici.

Questi cifrari utilizzano una serie di cifrari di Cesare intrecciati, rendendo la crittoanalisi molto più complessa.

Storia e Significato

- Per secoli considerato "le déchiffrable indéchiffrable" (il cifrario indecifrabile)
- Decifrato indipendentemente da Charles Babbage e Friedrich Kasiski
- Metodi per dedurre la lunghezza della parola chiave sviluppati con successo

Cifrario di Vigenère

Il cifrario di Vigenère utilizza una parola chiave per creare una serie di cifrari di Cesare intrecciati.

Tabella di Vigenère

A	B	C	D	E	F
A	B	C	D	E	F
B	C	D	E	F	G
C	D	E	F	G	H

01001001 01101110 01100110 01101111

01000001 01101100 01100111 01101111

01000100 01100101 01100011 01110010

2 – Crittografia Moderna

01010100 01100101 01100011 01101110

01000011 01110010 01101001 01110000

La Rivoluzione di Shannon

"Communication Theory of Secrecy Systems" (1949)

Claude E. Shannon ha introdotto una definizione formale di "sicurezza" nella crittografia, stabilendo le basi teoriche per la crittografia moderna.

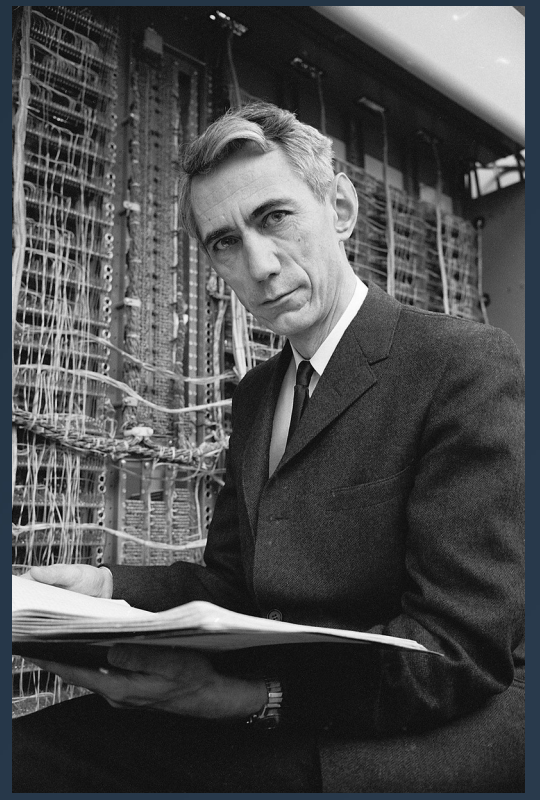
> *"La teoria dell'informazione ha trasformato la crittografia da una pratica basata su regole empiche a una scienza formale."*

Teoria della Informazione

Ha definito la quantità di informazione e il rumore nei sistemi di comunicazione.

Sicurezza Formale

Ha fornito criteri matematici per valutare la sicurezza dei cifrari.



Claude E. Shannon

"Padre dell'Età dell'Informazione"

Informazione Crittografia Teoria dei Codici

Crittografia Simmetrica Moderna

Evolutione dei Cifrari

- Passaggio dai cifrari classici agli algoritmi basati su operazioni binarie
- Introduzione di operazioni di permutazione e sostituzione complesse
- Standardizzazione dei processi crittografici

Concetto di Chiave Condivisa

Nella crittografia simmetrica, la stessa chiave viene utilizzata sia per la cifratura che per la decifratura.

Crittografia Trasmissione Decrittografia

Algoritmi Standard

DES

Data Encryption Standard (1977). Primo algoritmo standard a chiave simmetrica.

AES

Advanced Encryption Standard (2001). Attuale standard mondiale per la crittografia simmetrica.

Vantaggi e Limitazioni

Vantaggi

- ✓ Crittografia veloce

Limitazioni

- ✗ Distribuzione della chiave

Il Problema della Distribuzione delle Chiavi

Per n dispositivi, servono n(n-1)/2 canali sicuri per la distribuzione delle chiavi

Sfide Logistiche

Canali di comunicazione sicuri

La necessità di un canale segreto per ogni coppia di utenti.

Gestione delle chiavi

Ogni utente deve conservare e gestire chiavi simmetriche multiple.

Scalabilità

Il numero di chiavi cresce quadraticamente con il numero di utenti.

Questo problema ha portato alla ricerca di nuovi approchi crittografici...

La Rivoluzione della Chiave Pubblica

Il Problema

La crittografia simmetrica richiede che mittente e destinatario condividano una chiave segreta, complicato da distribuire in modo sicuro.

La Soluzione

La crittografia asimmetrica usa due chiavi diverse: una pubblica (conoscibile da tutti) e una privata (tenuta segreta).

Diffie-Hellman

Primo a proporre la idea della chiave pubblica nel 1976.

RSA

Algoritmo basato su fattorizzazione dei numeri primi.

Impatto

Ha rivoluzionato la crittografia.

Funzioni Hash e Firma Digitale

Funzioni Hash

- Proprietà di compressione: trasforma input di lunghezza variabile in output di lunghezza fissa
- Unicità: piccola modifica dell'input genera un output completamente diverso
- Applicazioni: memorizzazione sicura delle password, integrità dei dati

Firme Digitali

- Autenticazione: dimostra la provenienza del messaggio
- Integrità: garantisce che il messaggio non sia stato alterato
- Funzionamento: basato sulla crittografia a chiave pubblica

Verso la Blockchain

Il passaggio concettuale dalla crittografia tradizionale ai sistemi distribuiti basati su consenso rappresenta una rivoluzione nella storia della sicurezza delle informazioni.

Crittografia Tradizionale

- Chiavi simmetriche
- Trust centralizzato
- Crittografia a chiave privata

Blockchain

- Consensus distribuito
- Crittografia a chiave pubblica
- Registro immutabile

Consensus Distribuito

Meccanismi che consentono alla rete di raggiungere un accordo senza fiducia centralizzata.

Struttura a Catena

Blocco successivo a blocco, collegati in modo che ogni modifica richieda la computazione.

Bitcoin Whitepaper

Primo articolo a descrivere un sistema basato su blockchain per transazioni digitali.

01001001 01101110 01100110 01101111

01000001 01101100 01100111 01101111

01000100 01100101 01100011 01110010

3 – Criptovalute ed AI

01010100 01100101 01100011 01101110

01000011 01110010 01101001 01110000

Bitcoin: La Prima Criptovaluta

Il Whitepaper di Satoshi Nakamoto

Pubblicato nel 2008, il whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" ha introdotto una nuova forma di denaro elettronico basato esclusivamente su crittografia.

> *"Una banca elettronica basata sulla crittografia di tipo peer-to-peer che consente pagamenti diretti tra utenti senza intermediari."*

Innovazioni Crittografiche

Blockchain

Registro pubblico immutabile di tutte le transazioni Bitcoin.

Transazioni Sicure

Ogni transazione è protetta da crittografia e verificata da nodi di rete.

Consenso Distribuito

Algoritmi di consenso che garantiscono l'unicità delle monete.

Blockchain: Funzionamento e Caratteristiche

Struttura a Blocchi

I dati sono organizzati in blocchi concatenati in modo che ciascun blocco contenga un riferimento all'hash del blocco precedente, creando una catena immutabile.

Crittografia

Gli hash crittografici garantiscono l'integrità dei dati e la sicurezza della catena, rendendo difficile alterare i blocchi precedenti.

Proof-of-Work

Meccanismo di consenso che richiede di risolvere un problema computazionale complesso per aggiungere un nuovo blocco alla catena.

Consenso Distribuito

La rete di nodi convalida e replica la blockchain, garantendo decentralizzazione e resistenza alla censura.

Oltre Bitcoin: Evoluzione delle Criptovalute

Dopo Bitcoin, le criptovalute hanno evoluto verso nuove forme più avanzate, espandendo le possibilità dell'ecosistema blockchain.

Ethereum

- Prima implementazione di blockchain con smart contract
- Estendibilità tramite token ERC-20

Contratti Intelligenti

- Programmi che si eseguono automaticamente
- Eliminano la necessità di intermediari

Altre Innovazioni

Layer 2

Soluzioni per scalare le transazioni

DAO

Organizzazioni autonome

Stablecoins

Valute con valore stabile

Sicurezza Crittografica nelle Criptovalute

Curve Ellittiche

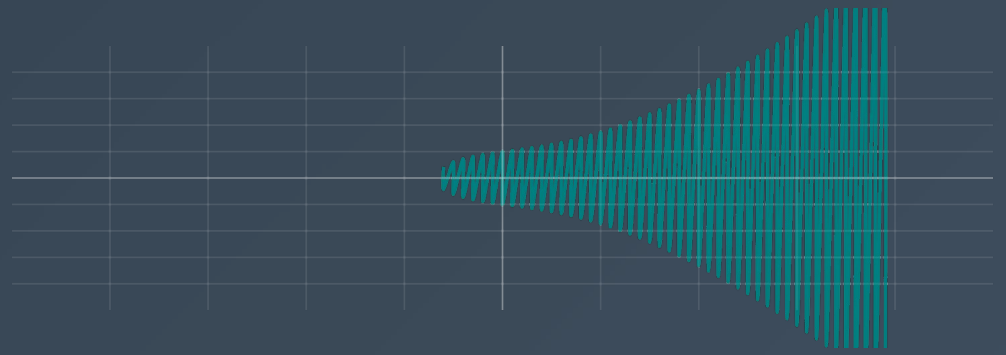
Base della sicurezza in molte criptovalute, offrendo maggiore protezione con chiavi più brevi.

Firme Schnorr

Sostituiscono le firme ECDSA, riducendo la dimensione delle firme e migliorando la privacy.

Altre Primitive

Funzioni hash crittografiche, alberi di Merkle e protocolli zero-knowledge.



Caratteristiche della Sicurezza

- Immutabilità delle transazioni
- Privacy e anonimato
- Consenso distribuito

Sfide di Sicurezza nell'Era Blockchain

Sebbene la blockchain offra una maggiore sicurezza rispetto ai sistemi tradizionali, presenta comunque sfide uniche che i crittoanalisti sfruttano.

Attacco del 51%

Quando un singolo attaccante o gruppo controlla più del 50% della potenza di hashing della rete, può manipolare le transazioni e impedire la conferma di altre transazioni.

Compromissione dei Wallet

La perdita o il furto di chiavi private porta alla perdita permanente dei fondi. I wallet online sono più vulnerabili agli attacchi rispetto a quelli offline.

Vulnerabilità dei Contratti Smart

Errori nel codice dei contratti possono essere sfruttati per prelevare fondi o interrompere il funzionamento del contratto.

Double Spending

Possibilità di spendere due volte lo stesso bitcoin, prima che la transazione venga confermata nella blockchain.

Misure di Sicurezza

- Utilizzo di chiavi cold storage
- Verifica della sicurezza dei contratti
- Implementazione di protocolli di consenso robusti

L'Impatto dell'IA sulla Crittografia

L'intelligenza artificiale ha un impatto duplice sulla crittografia: come strumento per migliorare i sistemi crittografici e come minaccia per la crittoanalisi.

Strumento per la Crittografia

- Automazione della crittoanalisi e ricerca di pattern
- Ottimizzazione degli algoritmi crittografici
- Generazione di chiavi più sicure tramite machine learning
- Rilevamento di anomalie nelle reti

Minaccia per la Crittografia

- Calcolo quantistico che mina la sicurezza dei cifrari tradizionali
- Analisi di pattern avanzate che potrebbero rivelare schemi nei cifrari
- Potenziale per breaking la crittografia simmetrica e asimmetrica
- Sfida per la crittoanalisi classica e moderna

L'evoluzione della crittografia deve tenere conto di questa duplice natura dell'IA.

Il Futuro: Crittografia Quantistica

La computazione quantistica rappresenta una minaccia significativa per i sistemi crittografici attuali, ma offre anche opportunità per algoritmi completamente nuovi e più sicuri.

Minaccia Quantistica

- Gli algoritmi classici (RSA, ECC) saranno vulnerabili
- Quantum computers possono fattorizzare in tempo polinomiale

Algoritmi Post-Quantistici

- Lattice-based, hash-based, multivariate
- Standardizzazione presso NIST

Crittografia Quantistica

- Utilizza principi quantistici per la sicurezza
- Key distribution basata su principi quantistici

Timeline

Attuale: alti costi di produzione per Q-transistor

Transizione: economia di scala per computer quantistici

Futuro: Q-transistor identici per dimensione a quelli binary

Conclusioni e Prospettive Future

Sintesi Evolutiva

Dai Cifrari Antichi

Dalla semplice sostituzione ai principi matematici complessi.

Crittografia Moderna

Da Shannon alla chiave pubblica, passando per i funzioni hash.

Blockchain e Criptovalute

Da Bitcoin a un ecosistema di tecnologie innovative.

Prospettive Future

Intelligenza Artificiale

- Crittografia quantistica contro attacchi di IA
- AI come strumento per migliorare la sicurezza

Crittografia Quantistica

- Base teorica: meccanica quantistica
- Sicurezza provata teoricamente

Riferimenti e Risorse

Libri e Pubblicazioni Accademiche

- "The Code Book" di Simon Singh
- "Crittografia Applicata" di Bruce Schneier
- "Bitcoin: The Protocol Handbook" di Amir Taaki

Siti Web e Forum

- Bitcoin.org - Documentazione
- Crypto.stackexchange.com
- Reddit: r/Cryptography, r/Bitcoin

Corsi Online

- Coursera: "Cryptography I" di Stanford
- edX: "Introduction to Cryptography"
- Udemy: "Bitcoin per Principianti"

Risorse per Criptovalute

- CoinDesk, Bitcoin Magazine
- Blockchain explorers (Bitcoin, Ethereum)
- Librerie per sviluppo crittografico

Papers di Ricerca

- Bitcoin whitepaper di Satoshi Nakamoto
- "A Mathematical Theory of Communication" di Shannon
- Preprint di ePrint (IACR)

Strumenti e Codice

- GitHub: repository crittografici
- Librerie: OpenSSL, Bouncy Castle
- Simulatori di blockchain