Triple DES (3-DES)

Cifratura a Blocchi e Sicurezza delle Informazioni

Prof. Fedeli Massimo

IIS Fermi Sacconi Cpia - Ascoli Piceno

3 gennaio 2026

Indice

Cos'è la Crittografia?

Definizione

La **crittografia** è la scienza che protegge le informazioni trasformandole in modo che solo chi possiede la "chiave" corretta possa leggerle.

Testo in chiaro:

CIAO MONDO

Testo cifrato:

X9K2 QW8RT5

Perché è importante?

- Protezione dei dati personali
- Sicurezza nelle transazioni online
- Protezione della privacy

Cifratura Simmetrica vs Asimmetrica

Cifratura Simmetrica

- **Una sola chiave** per cifrare e decifrare
- Più veloce
- Chiave segreta condivisa
- Es: DES, AES, 3-DES

Cifratura Asimmetrica

- **Due chiavi**: pubblica e privata
- Più lenta
- Chiave pubblica distribuita
- Es: RSA, ECC

3-DES è un algoritmo di cifratura SIMMETRICA

La Storia di DES

Data Encryption Standard (DES)

- Sviluppato da IBM negli anni '70
- Adottato come standard dal governo USA nel 1977
- Chiave di **56 bit** (effettivi, 64 bit totali con parità)
- Blocchi di **64 bit**

Il Problema di DES

Con l'aumento della potenza di calcolo dei computer, la chiave a 56 bit è diventata troppo **corta** e vulnerabile agli attacchi *brute force*.

Soluzione

Nel 1998 è stato dimostrato che DES poteva essere violato in meno di 3 giorni!
Necessaria una soluzione più sicura $\rightarrow$ 3-DES

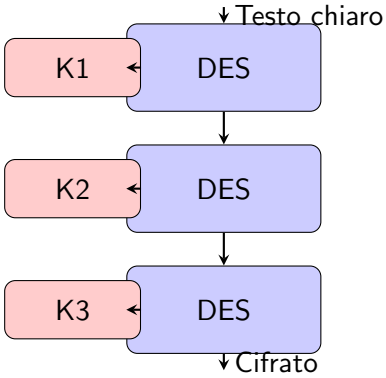
Perché Triple DES?

Problema:

- DES troppo debole (56 bit)
- Moltissimi sistemi già usavano DES
- Costoso cambiare tutto l'hardware

Soluzione Intelligente:

- Applicare DES **tre volte**
- Usare chiavi diverse
- Compatibilità con hardware esistente

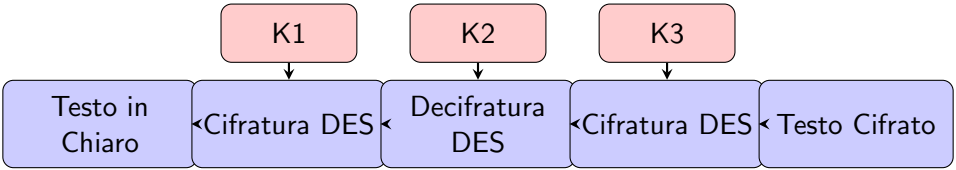


Schema EDE: Encrypt-Decrypt-Encrypt

Il Metodo Standard di 3-DES

3-DES utilizza lo schema **EDE** (Encrypt-Decrypt-Encrypt):

1. **Encrypt** con chiave K1
2. **Decrypt** con chiave K2
3. **Encrypt** con chiave K3



Perché Decrypt al centro?

Permette la **retrocompatibilità** con DES: se K1 = K2 = K3, otteniamo il DES originale!

Le Tre Opzioni di Chiavi

3-DES può essere configurato in tre modi diversi:

Opzione 1: Tre chiavi distinte (3TDES - Keying Option 1)

K1 $\neq$ K2 $\neq$ K3
Sicurezza: 168 bit (3×56)
Più sicuro ma meno usato

Opzione 2: Due chiavi distinte (3TDES - Keying Option 2)

K1 = K3 $\neq$ K2
Sicurezza: 112 bit (2×56)
Più comune - buon compromesso sicurezza/efficienza

Opzione 3: Una chiave (retrocompatibilità)

K1 = K2 = K3
Sicurezza: 56 bit

Esempio Pratico: Opzione 2

Scenario Reale (Opzione 2: K1 = K3)

1. **Chiavi:**
   - K1 = K3 = `0x133457799BBCDFF1`
   - K2 = `0x0E329232EA6D0D73`

2. **Testo in chiaro:**

   `"HELLO___"` (64 bit = 8 caratteri)

3. **Processo:**
   - Cifratura DES con K1 → `X1`
   - Decifratura DES con K2 su X1 → `X2`
   - Cifratura DES con K3 su X2 → **Testo Cifrato**

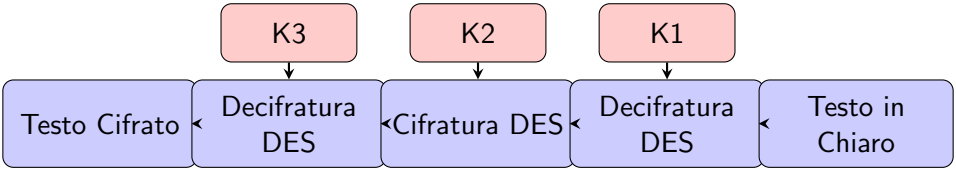
Il processo inverso permette di recuperare il testo originale

Decifratura con 3-DES

Il Processo Inverso

Per decifrare, si inverte l'ordine e si scambiano cifratura con decifratura:

1. **Decrypt** con chiave K3
2. **Encrypt** con chiave K2
3. **Decrypt** con chiave K1



Quanto è Sicuro 3-DES?

Punti di Forza

- Chiavi lunghe: fino a 168 bit
- Testato per decenni
- Nessun attacco pratico conosciuto
- Ampiamente certificato

Limitazioni

- Più lento di AES (3x operazioni)
- Blocchi piccoli (64 bit)
- Birthday attack dopo 2^{32} blocchi
- Deprecato dal NIST (2023)

Attacco Meet-in-the-Middle

Riduce la sicurezza effettiva:

- 3 chiavi: da 168 a **112 bit**
- 2 chiavi: da 112 a **80 bit**

Tempo per Violazione

Con tecnologia attuale:

- 112 bit: **milioni di anni**
- 80 bit: ancora **impraticabile**

Confronto: 3-DES vs AES

Caratteristica	3-DES	AES
Anno di sviluppo	1978/1998	2001
Dimensione chiave	112-168 bit	128/192/256 bit
Dimensione blocco	64 bit	128 bit
Velocità	Lenta (3× DES)	Veloce
Sicurezza	Buona ma limitata	Eccellente
Hardware richiesto	Maggiore	Minore
Status	Deprecato (2023)	Standard attuale
Uso consigliato	Solo legacy	Raccomandato

Raccomandazione

Per nuovi sistemi: usare **AES**!

3-DES solo per mantenere compatibilità con sistemi esistenti.

Dove si Usa 3-DES?

Sistemi Finanziari

- **Carte di credito/debito**
- Bancomat (ATM)
- Transazioni POS
- Standard EMV (chip)
- Bonifici bancari

Telecomunicazioni

- Protocolli VPN legacy
- Crittografia voce
- Reti private

Compatibilità Legacy

- Sistemi governativi vecchi
- Hardware industriale
- Protocolli di sicurezza esistenti
- Database cifrati

Transizione in Corso

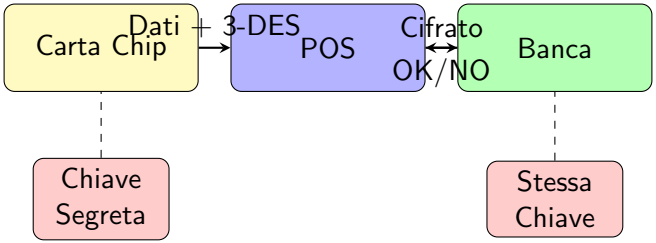
Molti sistemi stanno migrando da 3-DES ad AES per:

- Maggiore velocità
- Migliore sicurezza
- Minor consumo energetico

Esempio: Pagamento con Carta

Il Processo di una Transazione

1. Inserisci la carta nel POS
2. Il chip genera un codice crittografico con **3-DES**
3. Il codice viene inviato alla banca
4. La banca verifica usando la stessa chiave
5. Transazione autorizzata o rifiutata



La Fine di 3-DES

Deprecazione Ufficiale

- **2017**: NIST annuncia la dismissione
- **2023**: Fine del supporto ufficiale
- **2024-2030**: Periodo di transizione

Perché?

- Blocchi troppo piccoli (64 bit)
- Vulnerabilità Sweet32
- Prestazioni inadeguate
- Alternative migliori (AES)

Migrazione

Passaggio ad AES:

- AES-128: standard
- AES-256: alta sicurezza
- Hardware moderno
- Supporto software

3-DES: 45 anni di servizio onorevole!

Conclusioni

Cosa Abbiamo Imparato

- 3-DES è una **evoluzione** di DES per aumentare la sicurezza
- Usa tre applicazioni di DES con chiavi diverse (schema EDE)
- Offre sicurezza tra 80 e 112 bit (effettivi)
- È stato fondamentale per la sicurezza delle transazioni finanziarie
- Oggi è in fase di dismissione a favore di AES

Lezione Importante

La crittografia è un campo in **continua evoluzione**:

- Ciò che è sicuro oggi potrebbe non esserlo domani
- È necessario aggiornare costantemente i sistemi
- La sicurezza richiede attenzione e manutenzione

Domande per Riflettere

1. Perché non si è semplicemente raddoppiata la lunghezza della chiave di DES invece di applicarlo tre volte?
2. Se 3-DES è più sicuro, perché si preferisce AES per i nuovi sistemi?
3. Cosa succederebbe se qualcuno scoprisse la tua chiave 3-DES?
4. Come pensi che la crittografia dovrà evolversi con l'arrivo dei computer quantistici?

Grazie per l'attenzione!

Risorse per Approfondire

Standard e Documentazione

- NIST Special Publication 800-67: Recommendation for Triple DES
- ISO/IEC 18033-3: Encryption algorithms

Libri Consigliati

- "Applied Cryptography" - Bruce Schneier
- "Cryptography and Network Security" - William Stallings

Risorse Online

- Khan Academy - Cryptography Course
- Coursera - Cryptography (Stanford University)
- CryptoHack - Esercizi pratici interattivi