CRITTOGRAFIA E CALCOLO

Collegamenti per l'Esame di Stato

MATEMATICA - Integrali Definiti

Definizione Fondamentale

L'**integrale definito** ∫[a,b] f(x)dx è l'**area S compresa tra la funzione f(x) e l'asse delle ascisse**, delimitata dai segmenti verticali x=a e x=b.

Costruzione tramite Somme di Riemann

Processo di approssimazione:

1. **Suddividiamo** l'intervallo [a,b] in n parti uguali di ampiezza Δx
2. **Calcoliamo** la somma delle aree dei rettangoli: S ≈ Σ f(xi) · Δx
3. **Al limite** per n → ∞, otteniamo l'area esatta:

   lim(n→∞) Σ f(xi) · Δx = ∫[a,b] f(x)dx

Concetto chiave: L'integrale **trasforma infinite parti infinitesime in una totalità finita**.

Teorema Fondamentale del Calcolo Integrale

Se F(x) è una primitiva di f(x), allora: **∫[a,b] f(x)dx = F(b) - F(a)**

Questo collega derivate e integrali: per calcolare l'area, basta trovare la primitiva.

Teorema del Valor Medio Integrale

Se f(x) è continua su [a,b], **esiste almeno un punto c ∈ [a,b]** tale che:

∫[a,b] f(x)dx = f(c) · (b-a)

Interpretazione geometrica: L'area sotto la curva equivale all'area di un **rettangolo di base (b-a) e altezza f(c)**.

Collegamento Crittografico: Distribuzione dei Numeri Primi

Teorema dei Numeri Primi: La densità dei numeri primi intorno a n è approssimativamente 1/ln(n).

Applicazione dell'integrale: Per stimare quanti numeri primi ci sono nell'intervallo [a,b]: **π(b) - π(a) ≈ ∫[a,b] 1/ln(x) dx**

Il **teorema del valor medio** garantisce che esiste un punto c dove la densità 1/ln(c) è **rappresentativa dell'intero intervallo** - questo è cruciale per la sicurezza crittografica, perché assicura una distribuzione uniforme dei primi.

SISTEMI E RETI - Crittografia

Perché i Numeri Primi nella Crittografia?

Teorema Fondamentale dell'Aritmetica

Ogni numero intero > 1 ha una **fattorizzazione unica** in numeri primi:

- $12 = 2^2 \times 3$
- $77 = 7 \times 11$
- $1001 = 7 \times 11 \times 13$

Principio di sicurezza: Moltiplicare è facile, fattorizzare è difficilissimo.

Piccolo Teorema di Fermat

Se p è primo e a non è divisibile per p: **a^(p-1) ≡ 1 (mod p)**

Le potenze "ritornano" sempre a 1 - questo crea cicli matematici perfetti per cifratura/decifratura.

Algoritmo RSA - Passo per Passo

Generazione Chiavi:

1. **Scegli** due primi molto grandi: p, q (es. p=1009, q=1013)
2. **Calcola** n = p × q = 1,022,117
3. **Calcola** φ(n) = (p-1)(q-1) = 1008 × 1012 = 1,020,096
4. **Scegli** e coprimo con φ(n), spesso e = 65537
5. **Calcola** d tale che e × d ≡ 1 (mod φ(n))

Cifratura/Decifratura:

- **Chiave pubblica**: (n, e)
- **Chiave privata**: (n, d)
- **Cifratura**: c ≡ m^e (mod n)

- **Decifratura**: m ≡ c^d (mod n)

Sicurezza: Senza conoscere p e q, è impossibile calcolare φ(n) e quindi d.

Diffie-Hellman - Scambio Sicuro

Protocollo:

1. **Accordo pubblico**: primo p e radice primitiva g
2. **Alice**: sceglie segreto a, calcola A = g^a mod p
3. **Bob**: sceglie segreto b, calcola B = g^b mod p
4. **Scambio pubblico**: Alice e Bob si inviano A e B
5. **Chiave comune**:
   - Alice: K = B^a mod p = g^(ba) mod p
   - Bob: K = A^b mod p = g^(ab) mod p

Problema del Logaritmo Discreto

Dato g^a mod p, calcolare a è computazionalmente impossibile per primi grandi.

SSL/TLS - Combinazione Perfetta

Handshake: Usa Diffie-Hellman per scambiare chiavi **Sessione**: Usa crittografia simmetrica (AES) con le chiavi scambiate **Autenticazione**: Usa RSA per certificati digitali

Collegamento matematico: Come l'integrale accumula infiniti contributi per ottenere un risultato finito, la crittografia accumula bit di casualità (dai primi) per costruire sicurezza totale e inviolabile.

STORIA - Seconda Guerra Mondiale

Decrittazione di Enigma

Contesto: La macchina Enigma tedesca cifrava messaggi militari con trilioni di combinazioni possibili.

Breakthrough:

- **Bletchley Park** (Regno Unito)
- Team di matematici e crittanalisti
- Utilizzo di macchine "Bombe" per testare combinazioni
- Sfruttamento di pattern ricorrenti nei messaggi

Impatto: La decrittazione accorciò la guerra di 2-4 anni, salvando milioni di vite.

Collegamento: Come il valor medio trova il punto rappresentativo, i crittoanalisti trovavano schemi ricorrenti per "rompere" i codici.

INGLESE - Alan Turing

Biografia e Contributi

Alan Turing (1912-1954): Matematico britannico, padre dell'informatica moderna.

Macchina di Turing: Modello teorico che definisce cosa significa "calcolare".

- **Nastro infinito** con simboli
- **Testina** che legge/scrive
- **Stati finiti** che determinano le azioni

Test di Turing

Criterio per determinare se una macchina possiede intelligenza: se un umano non riesce a distinguere le risposte della macchina da quelle umane.

Ruolo in WW2

Leader del team che decrittò Enigma a Bletchley Park.

Collegamento: Turing applicò il rigore matematico (come negli integrali) per risolvere problemi crittografici concreti.

INFORMATICA - Sicurezza Database

Vincoli di Integrità

Referenziale: Le chiavi esterne devono corrispondere a chiavi primarie esistenti. **Sui Domini**: I valori devono rispettare i tipi definiti. **Sulle Tuple**: Vincoli che coinvolgono più attributi.

Sicurezza SQL

Controllo Accessi: GRANT/REVOKE per gestire privilegi. **SQL Injection**: Attacco che sfrutta input non validati. **Crittografia**: Campi sensibili cifrati nel database.

Collegamento: Come l'integrale garantisce la "totalità" di un calcolo, i vincoli garantiscono l'integrità totale dei dati.

TPS - GDPR, AI e Sicurezza Digitale

Il Flusso della Sicurezza Digitale

RSA → Certificati Digitali ← Diffie-Hellman → SSL/TLS

Certificati Digitali - La Catena di Fiducia

Struttura di un Certificato X.509:

1. **Chiave pubblica** del soggetto (RSA/ECDSA)
2. **Identità** del proprietario (CN, O, C)
3. **Firma digitale** dell'Autorità di Certificazione (CA)
4. **Periodo di validità** (not before/not after)
5. **Algoritmi** di hash e cifratura utilizzati

Processo di Verifica:

1. **Estrazione** della chiave pubblica della CA
2. **Verifica** della firma digitale sul certificato
3. **Controllo** della catena di certificazione fino alla Root CA
4. **Validazione** delle date e dello stato di revoca (CRL/OCSP)

Principio matematico: La firma usa RSA per garantire **integrità** e **autenticità** - nessuno può falsificare un certificato senza la chiave privata della CA.

GDPR e AI Act - Framework di Sicurezza

GDPR - Principi Fondamentali:

- **Minimizzazione**: Raccogliere solo dati necessari
- **Trasparenza**: Informare sui trattamenti
- **Sicurezza**: Proteggere con **misure tecniche adeguate** (crittografia)
- **Accountability**: Dimostrare la conformità

AI Act - Classificazione dei Rischi:

- **Inaccettabile**: Sistemi che manipolano comportamenti
- **Alto Rischio**: Sistemi in settori critici (sanità, trasporti)
- **Limitato**: Chatbot con obblighi di trasparenza
- **Minimo**: Nessun obbligo specifico

Collegamento: Il **machine learning** per i sistemi AI richiede **markup** di dati personali → necessità di **crittografia** end-to-end.

Fatturazione Elettronica - XML e Sicurezza

Processo Completo:

1. **Generazione XML**: Documento strutturato secondo standard FatturaPA
2. **Firma Digitale**: Applicazione di firma PKCS#7 (usa RSA)
3. **Validazione**: Controllo formato, contenuto e firma
4. **Trasmissione**: Invio sicuro tramite **SdI** (Sistema di Interscambio)

Struttura XML Base:

```
<FatturaElettronica>
  <FatturaElettronicaHeader>
    <DatiTrasmissione>
      <CodiceDestinatario>ABC123</CodiceDestinatario>
    </DatiTrasmissione>
  </FatturaElettronicaHeader>
  <FatturaElettronicaBody>
    <DatiGenerali>...</DatiGenerali>
  </FatturaElettronicaBody>
</FatturaElettronica>
```

Sicurezza del Processo:

- **Integrità**: Hash SHA-256 del documento
- **Autenticità**: Firma digitale RSA del mittente
- **Non ripudio**: Timestamp qualificato
- **Riservatezza**: Trasmissione su canali cifrati (TLS)

Framework di Sicurezza Generale

Livelli di Protezione:

1. **Trasporto**: SSL/TLS per comunicazioni
2. **Applicativo**: Autenticazione e autorizzazione
3. **Dati**: Crittografia dei campi sensibili
4. **Processo**: Audit trail e logging sicuro

Principio dell'Accumulo di Sicurezza:

Come l'**integrale definito** accumula contributi infinitesimi per ottenere un'area totale, la sicurezza digitale accumula:

- **Bit di entropia** (casualità crittografica)
- **Livelli di validazione** (certificati, hash, firme)
- **Controlli di conformità** (GDPR, AI Act)
- **Misure tecniche** (TLS, XML Schema, audit)

Risultato finale: Un ecosistema digitale sicuro dove ogni componente contribuisce alla **protezione totale** dei dati e dei processi.

ITALIANO - Svevo e l'Integrazione dell'Inconscio

Italo Svevo - La Coscienza di Zeno

Romanzo psicoanalitico che esplora l'inconscio del protagonista.

Tecnica Narrativa:

- **Flusso di coscienza**
- **Tempo misto** (presente/passato)
- **Inaffidabilità del narratore**

Psicoanalisi Freudiana

Influenza delle teorie di Freud sulla letteratura:

- **Inconscio**: Territorio nascosto della mente
- **Rimozione**: Meccanismi di difesa
- **Transfert**: Rapporto analista-paziente

Collegamento Matematico-Letterario

Metafora dell'Integrazione: Come l'integrale definito "raccoglie" tutti i contributi infinitesimi per ottenere un risultato totale, la psicoanalisi raccoglie frammenti dell'inconscio per "integrare" la personalità del paziente.

Zeno cerca di integrare i suoi ricordi frammentari in una narrazione coerente, proprio come l'integrale unifica punti discreti in una curva continua.

SINTESI DEI COLLEGAMENTI

Tema Unificante: **ACCUMULO E TOTALITÀ**

1. **Matematica**: L'integrale accumula contributi infinitesimi
2. **Crittografia**: Accumula bit di casualità per sicurezza totale
3. **Storia**: Accumulo di decrittazioni per vincere la guerra
4. **Turing**: Accumulo di calcoli per simulare l'intelligenza
5. **Database**: Accumulo di vincoli per integrità totale
6. **GDPR**: Accumulo di misure per protezione totale
7. **Svevo**: Accumulo di ricordi per coscienza totale

Frase Chiave

"Come l'integrale definito trasforma infinite parti infinitesime in una totalità significativa, ogni disciplina cerca il proprio metodo per integrare frammenti dispersi in una comprensione completa: dalla sicurezza crittografica alla coscienza umana."