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

La Guerra delle Code: WW2 come Scontro Crittografico

Prima Guerra Mondiale vs Seconda Guerra Mondiale

WWI (1914-1918): Guerra di **trincea**, statica, logoramento fisico **WWII (1939-1945)**: Guerra **lampo**, dinamica, battaglia dell'informazione

Fattore decisivo WW2: Non solo forza militare, ma **superiorità crittografica**

L'Asse e i Codici: Germania, Italia, Giappone

Germania - Enigma

Macchina Enigma:

- **3-4 rotori** intercambiabili
- **26 lettere → trilioni di combinazioni**
- **Chiave giornaliera** diversa per ogni unità
- **Fiducia cieca**: "Mathematisch unmöglich" (matematicamente impossibile da decifrare)

Vulnerabilità scoperte:

1. **Pattern umani**: Messaggi iniziavano spesso con "WETTER" (meteo)
2. **Errori operativi**: Riuso di chiavi, messaggi ripetuti
3. **Intercettazioni polacche**: Prime intuizioni sui rotori

UK - Bletchley Park: La Controffensiva

Colossus e Bombe:

- **Alan Turing** e team di matematici
- **10.000 persone** al lavoro sui codici
- **Macchine proto-computer** per testare combinazioni
- **Ultra**: Nome in codice per le decrittazioni

Impatto strategico:

- **Battaglia dell'Atlantico**: Localizzazione U-Boot tedeschi
- **Sbarco in Normandia**: Informazioni sui movimenti nemici
- **Accorciamento guerra**: Stimato 2-4 anni in meno

USA e il Progetto Manhattan: Sicurezza Atomica

Compartimentazione dell'Informazione

Principio: Ogni scienziato conosceva solo la propria parte

- **Los Alamos**: Assemblaggio finale
- **Oak Ridge**: Arricchimento uranio
- **Hanford**: Produzione plutonio

Crittografia interna:

- **Codici speciali** per comunicazioni tra siti
- **Telefoni cifrati** per coordinamento
- **Nomi in codice**: "Little Boy", "Fat Man"

Russia: Decrittazione e Controspionaggio

Venona Project (scoperto dopo guerra)

Gli **USA decrittarono** le comunicazioni sovietiche durante la guerra, scoprendo:

- **Spie atomiche**: Klaus Fuchs, David Greenglass
- **Infiltrazioni** nei progetti segreti alleati
- **Doppio gioco**: Alleati di guerra, nemici informativi

Futurismo e Nazismo: Tecnologia come Arma

Connessione con il Programma di Italiano

Marinetti e il Futurismo (programma svolto):

- **Celebrazione della tecnologia** e della velocità
- **"Zang Tumb Tumb"**: Onomatopee della guerra moderna
- **Influenza sul fascismo**: Estetica della potenza tecnologica

Parallelo storico: Come i futuristi esaltavano la "bellezza della guerra moderna", i nazisti credevano nella **superiorità tecnologica** come destino. L'Enigma rappresentava questa fiducia cieca nella perfezione tecnica.

L'Accumulo di Intelligence: Metodo dell'Integrale

Processo di Decrittazione come Integrazione

1. **Intercettazione**: Raccolta di singoli messaggi (punti discreti)
2. **Analisi frequenziale**: Studio di pattern ricorrenti
3. **Correlazione**: Collegamento tra messaggi diversi
4. **Sintesi**: Ricostruzione del quadro strategico completo

Come l'integrale definito: Infinite intercettazioni parziali → comprensione totale della strategia nemica

Il Teorema del Valor Medio nella Storia

Ogni **breakthrough crittografico** rappresentava il "punto c" del teorema del valor medio:

- Un singolo momento decisivo (come la prima decrittazione Enigma)
- Che rivelava il valore "medio" di tutta l'intelligence nemica
- Permettendo di calcolare l'impatto totale sulla guerra

Lezioni per l'Era Digitale

Principi Eterni della Guerra dell'Informazione:

1. **Mai fidarsi di un solo sistema**: Diversificazione crittografica
2. **Il fattore umano è sempre il più debole**: Errori operativi decidono
3. **La matematica vince sulla presunzione**: Superiorità tecnica ≠ invincibilità
4. **L'informazione è potere**: Chi controlla i codici controlla la guerra

Collegamento con oggi: Gli stessi principi di **accumulo di intelligence** e **superiorità crittografica** che decisero la WW2 sono alla base della cybersecurity moderna e delle guerre informatiche contemporanee.

INGLESE - Alan Turing e la Rivoluzione Computazionale

Alan Turing (1912-1954): Founding Father of Computer Science

La Macchina di Turing - Modello Teorico

Componenti fondamentali:

- **Nastro infinito**: Memoria con celle contenenti simboli
- **Testina mobile**: Legge/scrive/muove sul nastro
- **Stati finiti**: Determinano l'azione da compiere
- **Tabella di transizione**: Regole input → output

Funzione matematica: $T(a,b) = (\sigma,\delta,P)$

- **a** = stato attuale
- **b** = simbolo letto
- **σ** = nuovo stato
- **δ** = simbolo scritto
- **P** = movimento (sinistra/destra)

Rivoluzione concettuale: Definì cosa significa **"calcolare"** - ogni problema computabile può essere risolto da una Macchina di Turing.

Il Test di Turing (!): Definire l'Intelligenza

Imitation Game (1950)

Setup:

- **Interrogatore umano** (C)
- **Computer** (A)
- **Umano di controllo** (B)

Processo:

1. C fa domande ad A e B tramite terminale
2. A (computer) cerca di convincere C di essere umano
3. B (umano) cerca di dimostrare la propria umanità
4. **Test superato**: Se C non riesce a distinguere A da B

Criterio: Una macchina possiede intelligenza se **non è distinguibile** da un essere umano nelle risposte.

Bletchley Park: Turing vs Enigma

Breaking the "Unbreakable" Code

Enigma challenges:

- **158 trilioni** di combinazioni possibili
- **Chiavi giornaliere** diverse per ogni unità
- **3-4 rotori** intercambiabili

Turing's breakthrough:

1. **Bombe machines**: Dispositivi elettromeccanici per testare combinazioni
2. **Crib analysis**: Sfruttamento di testi probabili nei messaggi
3. **Pattern recognition**: Identificazione di abitudini umane nei codificatori

Mathematical approach: Trasformò la decrittazione da **arte** a **scienza**, applicando rigore matematico al posto dell'intuizione.

CAPTCHA ↔ Test di Turing Inverso

Modern Reversal

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart):

- **Obiettivo opposto**: Verificare che l'utente sia umano, non una macchina
- **Metodi**: Immagini distorte, puzzle visivi, riconoscimento oggetti
- **Evoluzione**: Da testo distorto a reCAPTCHA con Google Street View

Paradosso moderno: Mentre Turing voleva dimostrare che le macchine potevano sembrare umane, oggi usiamo test per dimostrare che gli umani non sono macchine!

AI e Machine Learning: L'Eredità di Turing

Da "The Fun They Had" (Asimov) alla Realtà

Nel programma svolto: Asimov immaginava computer che insegnavano ai bambini **Oggi**: ChatGPT, Claude, sistemi AI che effettivamente "insegnano" e conversano

Evoluzione del Test di Turing:

- **1950**: Può una macchina sembrare umana?
- **2024**: Le macchine **superano** molti umani in compiti specifici

Computing e Cryptography: Il Doppio Binario

Turing's Dual Legacy:

1. **Theoretical Computer Science**: Macchina di Turing come modello universale
2. **Practical Cryptography**: Metodi concreti per rompere codici nemici

Modern encryption: I principi crittografici di Turing (pattern analysis, statistical methods) sono alla base degli algoritmi moderni:

- **RSA**: Usa la difficoltà computazionale (fattorizzazione)
- **AES**: Usa la confusione e diffusione (principi di Turing)

Steve Jobs e Alan Turing: Bridging Theory and Practice

Dal Programma di Inglese svolto:

Jobs (nel programma): Visionario che rese i computer accessibili **Turing**: Teorico che li rese possibili

Continuum storico:

- **Turing (1940s)**: "Can machines think?"
- **Jobs (1980s)**: "How can machines serve humans?"
- **AI Era (2020s)**: "How can machines collaborate with humans?"

Collegamento con l'Integrale: Accumulation of Intelligence

Machine Learning come Integrazione

Processo di apprendimento AI:

1. **Input continui**: Dati infiniti come punti discreti
2. **Processing**: Algoritmi che "integrano" pattern dai dati
3. **Output**: Conoscenza totale maggiore della somma delle parti

Come l'integrale definito: ∫[training data] learning_function(x)dx = **Artificial Intelligence**

Turing's insight: L'intelligenza emerge dall'**accumulo** di regole semplici, proprio come l'area emerge dall'accumulo di rettangoli infinitesimi.

Legacy per il XXI Secolo

Turing's Questions ancora attuali:

1. **Consciousness**: ChatGPT è davvero "intelligente" o solo simula?
2. **Computability**: Ci sono problemi che nemmeno l'AI può risolvere?
3. **Ethics**: Se le macchine pensano, hanno diritti?

Connessione con crittografia moderna: I metodi di Turing per analizzare Enigma sono gli stessi usati oggi per:

- **Analizzare** blockchain e cryptocurrency
- **Proteggere** comunicazioni digitali
- **Sviluppare** quantum cryptography

Il ponte perfetto: Da matematico teorico a eroe di guerra a padre dell'era digitale - Turing incarnò l'**integrazione** tra teoria pura e applicazione pratica che definisce la computer science moderna.

INFORMATICA - Sicurezza Database

Autorizzazioni, Vincoli e Ponti SQL

Sistema di Autorizzazioni

GRANT/REVOKE: Sistema per controllare chi può fare cosa

```
GRANT SELECT, INSERT ON tabella TO utente;
REVOKE DELETE ON tabella FROM utente;
```

Vincoli di Integrità - I "Ponti" tra Tabelle

1. Chiavi Primarie (PK):

- **Identificano univocamente** ogni riga
- **Non possono essere NULL**
- Una sola per tabella

2. Chiavi Esterne (FK) - I "Ponti":

- **Collegano** due tabelle
- Devono **referenziare** una PK esistente
- Mantengono la **coerenza referenziale**

Esempio pratico:

```
CREATE TABLE Ordini (
    id_ordine INT PRIMARY KEY,
    id_cliente INT,
    FOREIGN KEY (id_cliente) REFERENCES Clienti(id)
);
```

3. Vincoli di Integrità Referenziale:

- **CASCADE**: Se elimino il padre, elimino anche i figli
- **SET NULL**: Se elimino il padre, i figli diventano NULL
- **RESTRICT**: Non posso eliminare se ha figli

Sicurezza - Difendersi dagli Attacchi

SQL Injection - Il Nemico Principale

Problema: Input non validato che "rompe" la query

```
-- Query vulnerabile
SELECT * FROM utenti WHERE nome = '$input';


-- Input malevolo: '; DROP TABLE utenti; --
-- Risultato: SELECT * FROM utenti WHERE nome = ''; DROP TABLE utenti; --'
```

Soluzioni:

1. **Prepared Statements**: Query parametrizzate

2. **Validazione input**: Controlli sui dati inseriti
3. **Escape characters**: Neutralizzare caratteri speciali

Modello AAA per Sicurezza Database

1. **Autenticazione**: Chi sei? (login/password)
2. **Autorizzazione**: Cosa puoi fare? (GRANT/REVOKE)
3. **Audit**: Cosa hai fatto? (log delle operazioni)

Crittografia nei Database

Cifratura dei Campi Sensibili

```
-- Esempio di campo cifrato
CREATE TABLE utenti (
    id INT PRIMARY KEY,
    nome VARCHAR(50),
    password_hash VARCHAR(256), -- Hash SHA-256
    carta_credito VARBINARY(256) -- Campo cifrato AES
);
```

Livelli di Protezione:

1. **Trasporto**: Connessioni SSL/TLS al database
2. **Storage**: Cifratura dei file del database
3. **Applicativo**: Hash delle password, campi sensibili cifrati
4. **Backup**: Backup cifrati per proteggere i dati storici

Collegamento con l'Integrale

Principio dell'Accumulo di Sicurezza: Come l'integrale definito accumula infinite parti infinitesime per ottenere un'area totale, la sicurezza del database accumula:

- **Vincoli** che garantiscono coerenza punto per punto
- **Autorizzazioni** che controllano ogni singola operazione
- **Controlli** che validano ogni input
- **Audit** che traccia ogni azione

Risultato finale: Un database dove ogni singolo dato è protetto e l'**integrità totale** è garantita dalla somma di tutti i controlli, proprio come l'integrale garantisce il calcolo esatto dell'area totale.

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 - L'Integrazione dell'Io nella Modernità

Futurismo: Crittografia della Velocità

Marinetti e la Sintassi Cifrata

"Zang Tumb Tumb" (dal programma svolto):

- **Distruzione** della sintassi tradizionale
- **Parole in libertà**: Comunicazione "cifrata" che bypass la logica
- **Onomatopee**: Linguaggio "primitivo" ma più diretto

Collegamento con Enigma: Come i tedeschi credevano nella superiorità tecnologica, i futuristi credevano nella superiorità della **velocità** e della **macchina** sulla tradizione.

Ungaretti: L'Integrale dell'Esperienza di Guerra

L'Allegria: Minimalismo come Massima Intensità

"Mattina": *"M'illumino / d'immenso"*

- **Input minimale**: Due versi, sei parole
- **Output massimale**: Esperienza totale dell'esistenza
- **Come l'integrale**: Infinite parti infinitesime (parole) → totalità infinita (emozione)

"Veglia":

- **Situazione**: Tutta la notte su un morto
- **Linguaggio**: Essenziale, "cifrato" dal dolore
- **Risultato**: **Fratellanza universale** emerge dal particolare

"San Martino del Carso": *"Di queste case / non è rimasto / che qualche / brandello di muro"*

- **Distruzione fisica → Costruzione poetica**
- **Accumulo di macerie → Integrazione** in verso immortale

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