

MATematica

INTEGRALI =

↓
RIMANN (1859)

$$\int_a^b f(x) dx = [F(x)]_a^b = F(b) - F(a)$$

DEFINITO

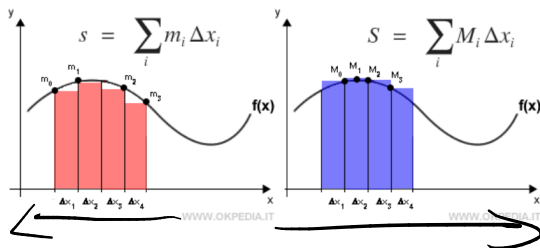
TRA a E b

→ SOMMA DI TUTTI GLI INTERVALLI

$$s = \sum m_i \Delta x_i \quad S = \sum M_i \Delta x_i$$

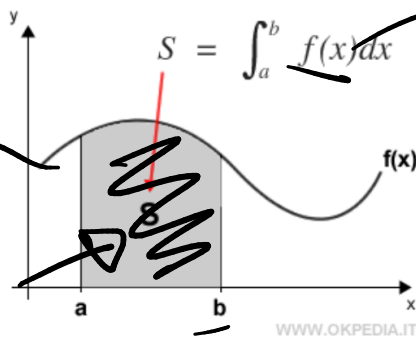
inferiore superiore

L'area della figura curvilinea è compresa tra la somma inferiore s e la somma superiore S .



RIMANN

INTEGRALE DEFINITO



F. INTEGRANDA

L'integrale definito di una funzione $f(x)$ in un intervallo $[a, b]$ è un numero reale che misura l'area S compresa tra la funzione e l'asse delle ascisse, delimitata dai due segmenti verticali che congiungono gli estremi $[a, b]$ al grafico della funzione.

CONTRARIO DI
DERIVATA =
PSINDESMO

ANSA TRA "a" E "b"

$[a, b]$

INT. CHIUSO

$$\lim_{\Delta x \rightarrow 0} s = \lim_{\Delta x \rightarrow 0} S = I \rightarrow \text{CONVERGONO AD } I = \text{INTEGRALE}$$

Al ridursi della base Δx i rettangoli diventano sempre più piccoli, riducendo la presenza delle superfici in difetto o in eccesso intorno al grafico.

L'integrale definito della funzione $f(x)$ nell'intervallo $[a, b]$ è indicato con la seguente notazione

$$I = \int_a^b f(x) dx$$

NUMERI REALI

→ CONCENTRATI IN DISTRIBUZIONI

TEOREMA

DEL VALORE MEDIO

Consideriamo una funzione $f: [a, b] \rightarrow \mathbb{R}$ limitata e integrabile in $[a, b]$. Si definisce media integrale (o valor medio) della funzione $f(x)$ sull'intervallo $[a, b]$ il numero reale:

$$M(f, [a, b]) = \frac{1}{b-a} \int_a^b f(x) dx$$

A parole il valore medio integrale non è altro che il rapporto tra l'integrale definito della funzione sull'intervallo e la lunghezza dell'intervallo stesso, intesa come differenza ordinata degli estremi.

5
257

↓

CRITTOGRAFIA

→ DIVISIBLER POR
50 50551
5 POR 1

- UNICI
- A UNA COSTA,
CONTINUANDO A DIVIDERE,
RITORNI AD 1
- FACILI IN PARTENZA,
DIFFICILI IN ARRIVO

NURSE
PANEL

RS 4.

DIFF 15 - 452 MAN

ALGORITMI A CRISTOLOGIA ASIMETRICA

1 CHAIN \rightarrow SIMULTANEA

2 CH₄N → ASIMOTRICA

$[A \xrightarrow{\text{CHAINS CORUS}} B]$

$$\left[\begin{array}{ccc} A & \xrightarrow{\text{conv.}} & B \\ \text{prev.} & & \text{prev.} \\ A & & B \end{array} \right]$$

RSA \rightarrow ASIMMETRICO

RUGST
SHANIR
ADUSMAN

RS A

INPUT : N, P, Q
(P, Q) - 3, 5

OUTPUT

N. FACILU $\rightarrow (3, 5)$

(M) $\rightarrow 133837$

N.
DIFFICUS \rightarrow 133837 \rightarrow GRAMS / SHEETS FOR
487 ACCANT

Generazione Chiavi:

1. Scegli due primi molto grandi: p, q (es. $p=1009, q=1013$)
2. Calcola $n = p \times q = 1,022,117$
3. Calcola $\varphi(n) = (p-1)(q-1) = 1008 \times 1012 = 1,020,096$
4. Scegli e coprimo con $\varphi(n)$, spesso $e = 65537$
5. Calcola d tale che $e \times d \equiv 1 \pmod{\varphi(n)}$

Cifratura/Decifratura:

- Chiave pubblica: (n, e)
- Chiave privata: (n, d)
- Cifratura: $c \equiv m^e \pmod{n}$
- Decifratura: $m \equiv c^d \pmod{n}$

DSA - ALGORITMO

$$(p, q) \rightarrow n = p \cdot q$$

$\varphi(n) \rightarrow$ ARITMETICA MODULARE
SULLO
 \downarrow
PRIMITIVA
1. 1009

MOD \rightarrow MODULO

$$4 \bmod 2 = 0$$

$$4/2 = 2$$

CON RESTO 0

$$\left[\begin{array}{l} 5 \bmod 2 = 1 \\ (2 \cdot 2) + 1 = 5 \end{array} \right]$$

DIFFIE - HELMAN

Diffie-Hellman - Scambio Sicuro

Protocollo:

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

Problema del Logaritmo Discreto

Dato $g^a \bmod p$, calcolare a è computazionalmente impossibile per primi grandi.

COMBINO N. PRIMI

CASI D'USO REALI:



COMUNICAZIONE DIGITALE

RSA

DIFFIE - HELMAN

ASIMMETRICO = HANDSHAKE

SSL/TLS

TPS



GDPR / AI

→ SICUREZZA = CERTIFICAZIONE [XML]

FRAMEWORK



USATO CORE

PASSO 1°

SICUREZZA

GENERARE ...

XML
LIBRO →
XML
LIBRO
TITOLO
PARAGRAFO
PARAGRAFO
TITOLO
LIBRO
(AUTENTICA: JSON)

MARKUP FOR
PERSONALIZZATO
= STRUTTURA
ADATTABILE

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

PROVIDER: ARUBA / POSNS

FIRMA DOCUMENTO

XML → X.509

FIRMA
DIGITALE

CRITOGRAFIA { C : CONFIDENZIALITÀ
I : INTEGRITÀ
A : DISPONIBILITÀ }

GDPR

2016 - EU

FIGURA:
DPO

=
DATA
PROTECTION
OFFICER

- ① MINIMIZZAZIONE DELLA RACCOLTA
- ② TRASPARENZA SUGLI FINI
- ③ RESPONSABILITÀ DEI DATI
- ④ RESPONSABILITÀ

→ REGOLAMENTO
PER RACCOLTA DATI ...

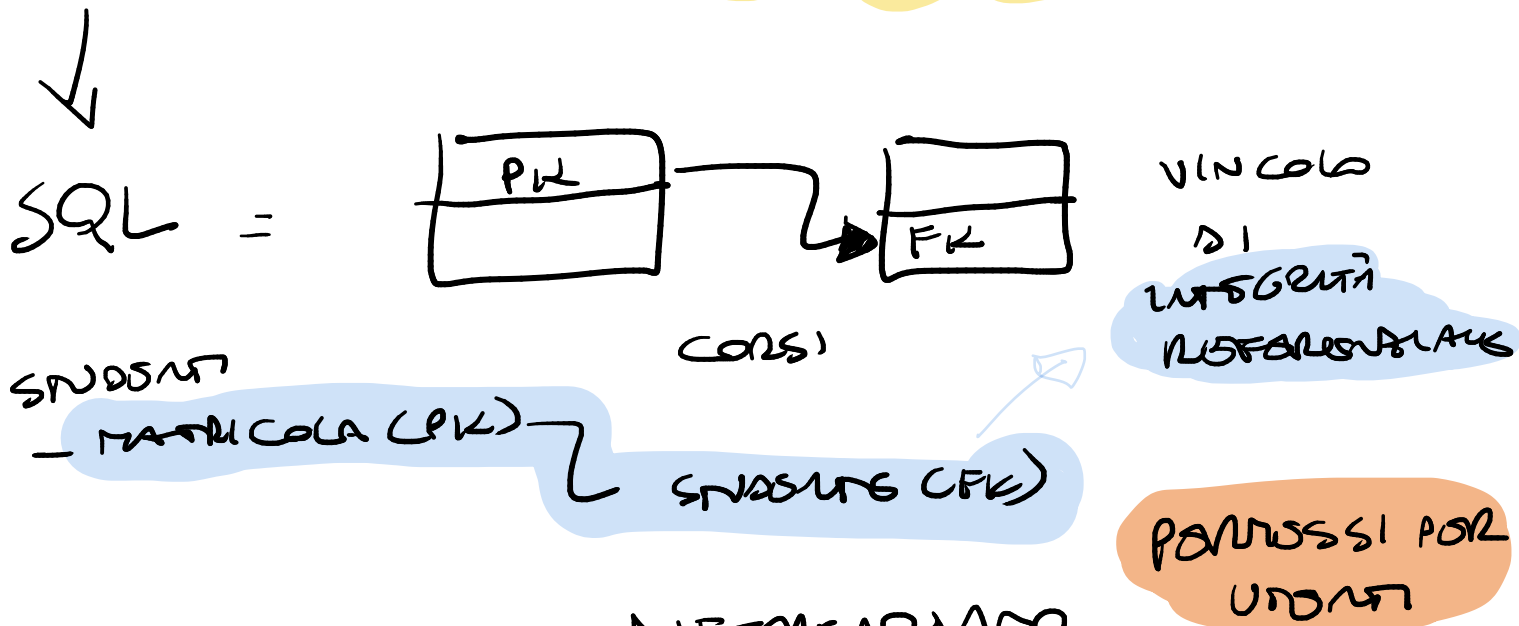
AI → AI ACT → EU

ETICA /
RACCOLTA DATI

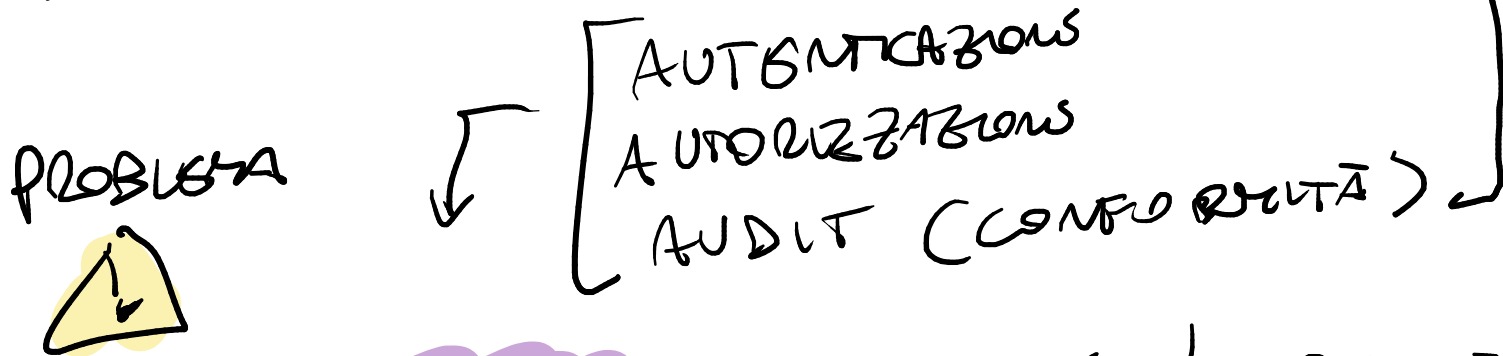
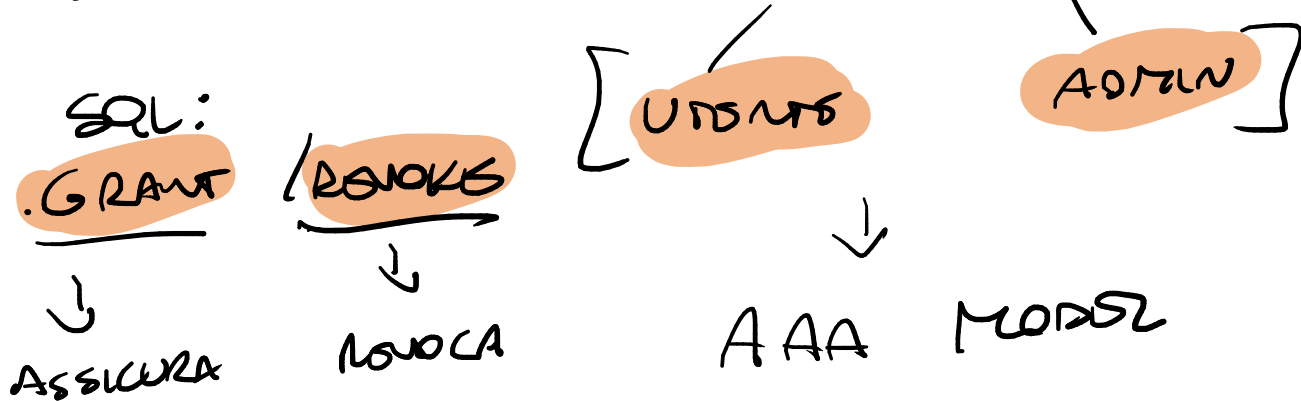
REGOLAMENTO PER
FINI DI
UTILIZZO
5 ART /
PIATTAFORMA AI

↓
SICUREZZA ? → PERMESSI ED
AUTORIZZAZIONI

INFORMAZIONE → AUTORIZZAZIONI, VINCOLI E PERMESSI

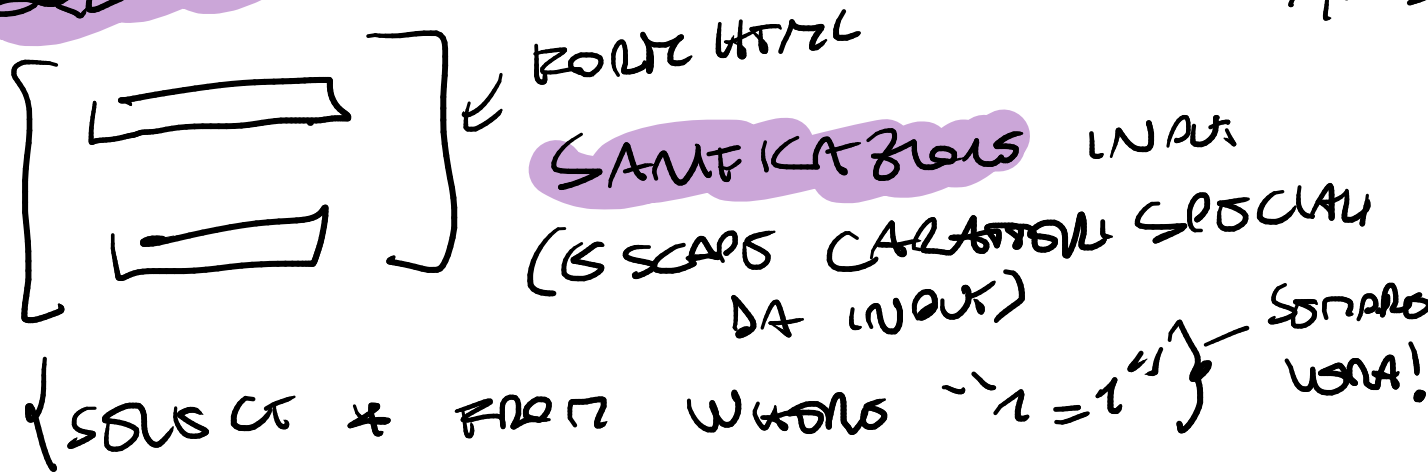


SICUREZZA → DIFFERENZIAMO



- SQL INJECTION

ESGOK = { 0...9 a...z
A...Z, !, ? } }



ENGLISH

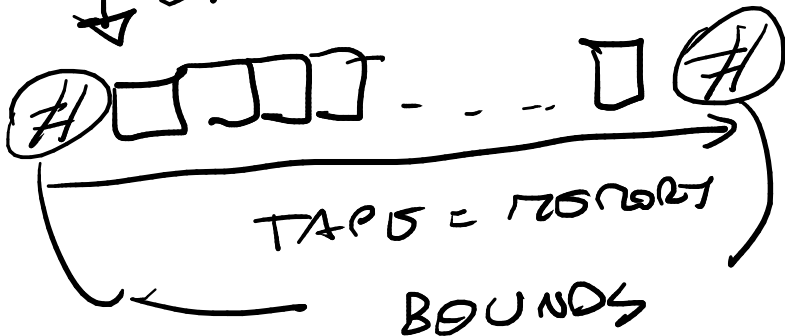
(ALAN TURING)

→ FOUNDED FATHER
OF COMPUTER SCIENCE

TURING MACHINES

→ FOUNDED MODEL
OF A COMPUTER

↓ = HEAD = READ / WRITES



$$\delta(q, a) = (t, b, R)$$

$$f(x) = y$$

INPUT → OUTPUT

- STATE FINITE → TERMINAL

- INPUT ($w \in \Sigma$) → OUTPUT

TESTING

AUTOMATIC =
INPUTS
DO GU INPUT

↓
SCARRO SU
NAGRO

CAPTCHA

TEST DI TURING (!)

TESTA IL TEMPO CHE CI
PUNTA A RISOLVERE
UN PROBLEMA

(
BOT
NON BOT

ENIGMA =

DESCRIZIONE
MESSAGGI
NABIST

[STORIA]



WW2 = SECONDA GUERRA MONDIALE

ENIGMA } UK
USA
RUSSIA

DECRYPT → GERMANIA
ITALIA
IMPERO AUSTRIACO
GIAPPONE

{ WW1 → GUERRA DI FRONDA
WW2 → GUERRA LAMPO / CARRI ARMATI
ANZI MODERNE }

RUSSIA → SPIONAGGIO

GERMANIA → RICERCA TECNOLOGICA
(MEDICINA ANZI VITA CORONA)

USA → PROGETTO MANHATTAN { USA
JAPAN }

OPPENHEIMER / FORNIT
PANISPERNA → ATOMICHE

[SBARCO DI NORMANDIA] ALLIATI VS. GERMANIA
(UK USA RUSSIA)

[ITALIANO]



TECNOLOGIA

FUTURISMO → PROPAGANDA MILITARE
MANIFESTI / PUBBLICITÀ

RAPIDITÀ



≅ UNGARETTI

GRUPTISMO



CONTO MA
DI UPRATTO

} MI ILUSTRINO
D'INTERESSO } MATTEO

SAN
MARTINO
DEL CARLO

USGUA

[The End → THAT'S ALL
BOYS!]