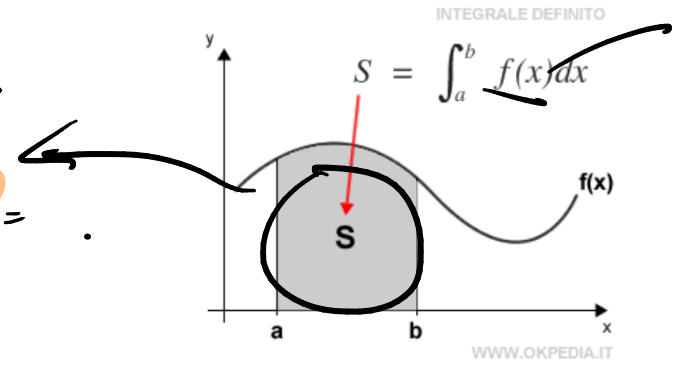
MATEMATICA

INTEGRALE =

↓

RIEMANN



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.

S = SOMMA

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

AREA TRA "a" E "b"

DEFINITO TRA a E b → SOMMA DI TUTTI GLI INFINITI

[a, b]

INT. CHIUSO

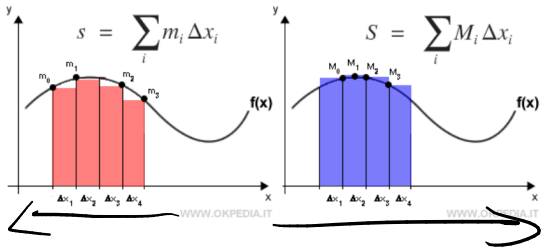
SUPERIORE

$S = \sum_i m_i \Delta x_i$ $S = \sum_i M_i \Delta x_i$

INFERIORE

$\lim_{\Delta x \to 0} s = \lim_{\Delta x \to 0} S = I$ → CONVERGE AD I = INTEGRALE

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



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

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

RIEMANN

NUMERI REALI → CONCENTRATI IN DISTRIBUZIONE

TEOREMA DEL VALOR MEDIO

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

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

INTEGRALE

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.

SISTEMI
E
RETI

↓

CRITTOGRAFIA

NUMERI PRIMI → DIVISIBILI PER SÉ STESSI E PER 1

- UNICI
- A UNA CERTA, CONTINUANDO A DIVIDERLI, RITORNI A 1
- FACILI IN PARTENZA, DIFFICILI IN ARRIVO

NUMERI PRIMI → [RSA, DIFFIE-HELLMAN] → ALGORITMI...

1 CHIAVE → SIMMETRICA → [A → B, CHIAVE COMUNE]

2 CHIAVI → ASIMMETRICA → [A → B, COMUNE; PRIV. A; PRIV. B]

RSA → ASIMMETRICO

RIVEST SHAMIR ADLEMAN

RSA → INPUT: N. PRIMI (P, Q) - 3, 5

OUTPUT:

(M) → 133837

N. FACILI → (3, 5)

N. DIFFICILE → 133837 → GRANDE / DIFFICILE PER ATTACCANTI

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)

RSA - ALGORITMO

(P, Q) → N = P · Q

φ_N → ARITMETICA MODULARE

EULERO

MOD → MODULO

4 MOD 2 = 0 4/2 = 2 CON RESTO 0

5 MOD 2 = 1

(2 · 2) + 1 = 5

DIFFIE - HELLMAN

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.

COMBINO N. PRIMI

CASI D'USO REALI:

CERTIFICATI DIGITALI

RSA → CERTIFICATI DIGITALI

DIFFIE-HELLMAN → SSL/TLS

TPS

GDPR / AI → SICUREZZA = CERTIFICATI [XML]

FRAMEWORK

USATO COME BASE PER SICUREZZA GENERALE ...

MARKUP PER FORMATO DATI PERSONALIZZATO = STRUTTURA TUA

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

XML → X.509

FIRMA DIGITALE

CRITTOGRAFIA

C : CONFIDENZIALITÀ

I = INTEGRITÀ

A = DISPONIBILITÀ

GDPR

2016 - EU

1. MINIMIZZAZIONE DELLA RACCOLTA
2. TRASPARENZA SULLE FINALITÀ
3. PORTABILITÀ DEI DATI DALLE PIATTAFORME
4. RESPONSABILITÀ

FIGURA: DPO = DATA PROTECTION OFFICER → REGOLAMENTO PER RACCOLTA DATI ...

AI → AI ACT → EU

ETICA / RACCOLTA DATI

REGOLAMENTO PER PIANI DI UTILIZZO 5 STATI / PIATTAFORME AI

SICUREZZA ? → PERMESSI ED AUTORIZZAZIONI

INFORMATICA → AUTORIZZAZIONI, VINCOLI E PARERI SSI