Interrogazione programmata di TPS e SISTEMI per Francesco Galiazzo.
Il programma di crittografia prevede:
Sicurezza e privacy, Fermat (che rivedremo martedi 19), trasmissione chiave, chiavi simmetriche e asimmetriche, aritmetica modulare.
Inoltre un argomento a piacere sul 4° livello OSI

SICUREZZA E PRIVACY

ES. TRASMISSIONE

A (ALICE) ⇄ B (BOB)

↑

CRITTOGRAFIA
(SCAMBIO DI DATI SICURO)

- **SIMMETRICA**

A ⇄ O B ← [PACCHETTO + CHIAVE]

(ALGORITMO) DI CRITTOGRAFIA

SIMMETRICA = A e B USANO LO STESSO ALGORITMO

MITTENTE → CRITTOGRAFIA → DESTINATARIO

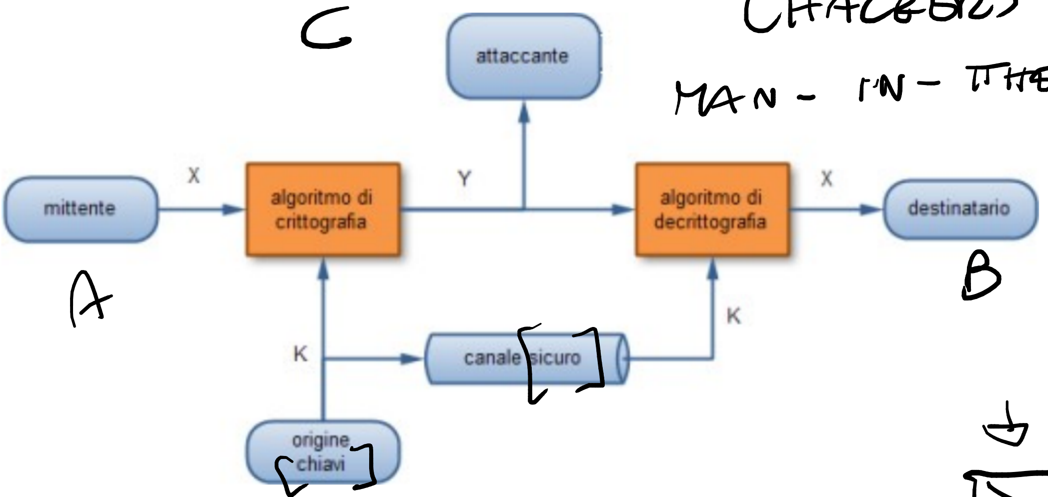
A — RSA/AES/ ... (ALGORITMI) — B

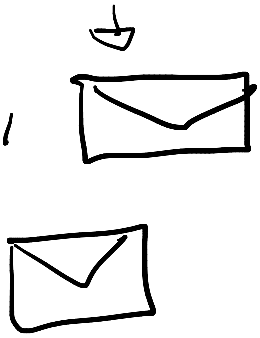
DECRITTOGRAFIA = LEGGERE IL PACCHETTO

[USO STESSO ALGORITMO PER]
- CRIPTARE (SICURO)
- DECRIPTARE (LO LEGGO)

MALINTENZIONATO (HACKER)

MAN-IN-THE-MIDDLE





A e B SI MANDANO MESSAGGI

C VUOLE LEGGERNE IL CONTENUTO

A ← C → B

[ARITMETICA MODULARE] → SOLO CHI È DENTRO LA TRASMISSIONE RIESCE A CAPIRE IL DATO!

[FORMULE O MODULI]

A e B si capiscono ma C non può (DECRITTOGRAFIA)

C → $\boxed{\text{ZIP}}$ → $\boxed{\text{ORIGINALE}}$

[NO TORNARE INDIETRO!]

MODULO →

$A \bmod B$ = resto + num. originale

[$\underbrace{5}_{A} \bmod \underbrace{2}_{B} = 1 * 2 = 2$
A e B]

ARITMETICA MODULARE → NUMERI CHE SI RIAVVOLGONO SU SÈ STESSI

$\equiv$ → CONGRUENZA

$A \equiv B$ A, B numeri

A / n
B / n → [LO STESSO NUMERO QUANDO DIVIDIAMO]

↓

STESSO RISULTATO !

FERMAT

[P = NUMERO PRIMO]

⇕

DIVISIBILE SOLO PER 1
O PER SÉ STESSO

= HA SENSO USARLI
PERCHÉ UN
ATTACCANTE DEVE
PROVARE TANTE COMBINAZIONI
PER ARRIVARE AL
MESSAGGIO

I numeri primi sono fondamentali nella crittografia moderna per due motivi principali:

1. Fattorizzazione difficile: È molto complesso scomporre in fattori primi un numero molto grande ottenuto dal prodotto di due numeri primi. Ad esempio, se moltiplico 997 × 991 = 987.827, per risalire ai fattori originali devo provare molte combinazioni.
2. Unicità: Ogni numero può essere scomposto in fattori primi in un solo modo, il che rende il sistema affidabile.

Fermat

Il piccolo teorema di Fermat dice che se p è un numero primo, allora per ogni intero a:

$$a^p \equiv a \pmod{p}$$

Questo significa che se si prende un qualunque numero a, lo si moltiplica per se stesso p volte e si sottrae a, il risultato è divisibile per p (aritmetica modulare).

È spesso espresso nella forma equivalente: se p è primo e a è un intero coprimo con p, allora:

$$a^{p-1} \equiv 1 \pmod{p}$$

Va notato che la prima espressione è in un certo senso più generale: è infatti valida per numeri interi arbitrari, come 0 o multipli di p, che invece non rientrano nelle ipotesi della seconda.

↑

METODO "SEMPLICE" PER GARANTIRE UNICITÀ NUMERI

INTERO A : S

$$a^p \equiv a \pmod p$$

CONGRUENZA

↓

$$5^3 \equiv 5 \pmod 3$$

$$125 \equiv 1 \qquad \begin{bmatrix} 125/1 = 125 \\ 1/1 = 1 \end{bmatrix}$$

[RITORNO AI N. DI PARTENZA!]

=

ARITM. MODULARE

FERMAT => ESSENDO UN ALGORITMO SEMPLICE, CI METTE "POCO" TEMPO

A cosa serve il Teorema di Fermat? E' molto utile per ridurre l'esponente nel calcolo delle potenze quando il numero è molto grande. L'unico limite è che si applica soltanto quando il modulo è un numero primo.

$$A \xrightarrow[\text{CHIAVE}]{} B$$

3 5 NUM. SEMPLICI

↓ ....

NUM. COMPOSTO [122878]

FERMAT $\Rightarrow$ MODO SEMPLICE PER A e B PER DECRIPTARE IL MESSAGGIO

(122878)

$\Downarrow$

(A/B) 3/5

SENSO PRATICO!

COROLLARIO:

$$a^p \equiv a \pmod p$$

e

$$a^{p-1} \equiv 1 \pmod p$$

SONO LA STESSA COSA

ARITM. MODULARE

- $a, b \in \mathbb{N}$, NUMERI INTERI
- $m \in \mathbb{N}$, MODULO

[NUMERO = NUMERO (OUTPUT)]

a mod m = resto divisione

a ≡ b mod m   significa   a mod m = b mod m

Proprietà aritmetica modulare:

[(a mod m) + (b mod m)] mod m = (a+b) mod m

[(a mod m) - (b mod m)] mod m = (a-b) mod m

[(a mod m) · (b mod m)] mod m = (a·b) mod m

[(a mod m)^k] mod m = a^k mod m

Esempi:

a = 6
b = 7
m = 5

→ VALORI CHE SCEGLI

→ [(a mod m) + (b mod m)] mod m = (a+b) mod m (ES. SOPRA = FORMULA)

[(6 mod 5) + (7 mod 5)] mod 5 = (6+7) mod 5 (SOSTITUZIONE)

(1 + 2) mod 5 = 13 mod 5

3 mod 5 = 13 mod 5

3 = 3

MOD = RESTO DIVISIONE

3 | 5 → 0.6...

7 | 5 → 1,... → RESTO 2

→ 0 + 3 = 3 (INTERO)

a = 8, b = 7, m = 5

[(a mod m) - (b mod m)] = (a - b) mod m

[(8 mod 5) - (7 mod 5)] = (8 - 7) mod 5

(3) (2) 1 mod 5

0.... +1 = 1.2 m / 1

8 | 5 → 1... +[3] = 8 RESTO

MODULO = PRENDO IL RESTO DELLA DIVISIONE

8 mod 5 = [1] [1.6] INTERO DECIMALE

1 mod 5

1/5 = 0.2

(0+1) · 1 = 1

→ 5 · (1) + [3] = 8

MODULO = NUMERO SOTTRATTO AL DIVIDENDO MI DÀ IL DIVISORE] DIVISIONE INTERA

$[3-2] = 1$

$[1 = 1] \rightarrow$ DIFFERENZA!

PRODOTTO $\rightarrow a / b / m = 8 / 7 / 5$

$(a \bmod m) \cdot (b \bmod m)^{\bmod m} = (a \cdot b) \bmod m$

$(8 \bmod 5) \cdot (7 \bmod 5)^{\bmod m} = (8 \cdot 7) \bmod 5$

$(3 \cdot 2)^{\bmod 5} = 56 \bmod 5 =$

$(6 \bmod 5) = (56 \bmod 5) \rightarrow 1 = 1$

$1 = 1$

Algoritmo di Diffie-Hellman

A e B conoscono due numeri g e p pubblici (p **primo** *cioè un numero naturale maggiore di 1 che sia divisibile solamente per 1 e per sé stesso*)

A conosce un numero segreto a

B conosce un numero segreto b

A calcola	$A = g^a \bmod p$	e lo comunica a	B
B calcola	$B = g^b \bmod p$	e lo comunica a	A
A calcola	$K = B^a \bmod p$		
B calcola	$K = A^b \bmod p$		

FORMULE

STESSO CONCETTO DI PRIMA CON FORMULE COMPLICATE

Ma:

$$K = B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ba} \bmod p$$
$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

A e B hanno condiviso un segreto (**il numero K**) senza comunicarlo esplicitamente!

Un eventuale attaccante può osservare A, B, g, p ma questa informazione non è sufficiente per ricavare K.

K è calcolabile solo conoscendo a o b, che tuttavia sono segreti e non vengono mai trasmessi. Ricavare a da A (o analogamente b da B) significa risolvere un logaritmo discreto, difficile dal punto di vista computazionale.