SISTEMI. Compito scritto in classe sui seguenti argomenti:
Inverso di e (mod f)
Algoritmo di Diffie-Hellman
Funzione di Eulero Φ(n)
Calcolare la chiave pubblica
Calcolare la chiave segreta d
Codificare e decodificare un messaggio m

[Inverso di e (mod f)] → RSA

Modulo → mod

a mod m = resto divisione

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

CONGRUENTE

ENTRAMBI DIVISIBILI

FUNZIONE DI EULERO

RESTO DIVISIONE

de ≡ 1 mod (p-1) (q-1)
de ≡ 1 mod φ(n)
de ≡ 1 mod f

φ = PHI = "FI"

de mod f = 1 mod f
**de mod f = 1**

COPRIMI = PRIMI TRA DI LORO

Conosco il numero **e**, conosco il numero **f** e so che sono [coprimi]

Numero primo = Divisibile per sé stessi e per 1

RSA →

- Scegliere **due numeri primi** **p e q** $p = 3,\ q = 5$
- Calcolare **n = pq** $n = 3 \cdot 5 = 13$
- Mediante la **f = φ(n) di Eulero** posso sapere quanti sono i numeri compresi tra 1 e n che siano coprimi con n e ne scelgo uno che chiamo **e**
- Calcolare l'**inverso (mod f)** di **e** che identifico con **d**
- La coppia **(n, e)** *è la **chiave pubblica***
- La coppia **(n, d)** *è la **chiave privata***
- Non è possibile risalire facilmente dalla chiave pubblica a quella privata (e viceversa), in quanto servirebbe conoscere il numero (p-1)(q-1), e questo implica fattorizzare n nei suoi fattori p e q (problema difficile)

Eulero:
- Serve a trovare il MCD (Massimo Comun Divisore) tra due numeri
  - I numeri coprimi (primi tra di loro)
  - Numeri primi (divisibili per sé stessi e per 1)
  - Es. 5 / 5 = 1 e 5 / 1 = 5

[ C'è un numero **d** tale che il **resto** della divisione **(d * e) / f** è **1**? ] → RESTO = 1

Per esempio prendiamo come numeri **e = 5** ed **f = 7**.
I due numeri sono coprimi perché il massimo comune divisore tra 5 e 7 è 1.
A questo punto arriva la domanda:

**C'è un numero d tale che il resto della divisione (d * 5) / 7 è 1?**

La risposta è **si**, e il numero **d** che cerchiamo è **3**.
Infatti **3 x 5 = 15, e il resto della divisione 3*5/7 è 1.**
Cioè **3*5 mod 7 = 1**

(7 · 2) + 1 = 15

Un modo sintetico per dire che "**il resto della divisione (d * e) / f è 1**" è il seguente:
"**d è l'inverso di e (mod f)**" o "**d è l'inverso (mod f) di e**".

Di seguito alcuni esempi:

- l'inverso (mod 7) di 5 è 3 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 3 è 5 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 6 è 6 perché 6 x 6 = 36 e 36(mod 7) = 1
- l'inverso (mod 43) di 11 è 4 perché 11 x 4 = 44 e 44(mod 43) = 1

l'inverso (mod 12) di 3 NON c'è perché il massimo comune divisore tra 12 e 3 è diverso da 1

```
Eulero - Dato il prodotto n = p * q (p, q primi)

- Φ(n) = (p-1)(q-1)

Ti viene dato n = 15 e trovi (3, 5 primi)

- Φ(15) = (3 - 1)(5 - 1)
- Φ(15) = 2 * 4 = 8
```

1 a 8 NUMERI COPRIMI

- Scegliere **due numeri primi p e q** `p = 3, q = 5`
- Calcolare **n = pq** `n = 3 * 5 = 15`
- Mediante la **f = φ(n) di Eulero** posso sapere quanti sono i numeri compresi tra 1 e n che siano coprimi con n e ne scelgo uno che chiamo **e** `Φ(15) = 8 = Numeri coprimi compresi tra 1 e 8`
- Calcolare l'**inverso (mod f)** di **e** che identifico con **d** `inverso (mod 15) di 2 = 7`
- La coppia **(n, e)** = `(15, 2)` *è la **chiave pubblica***
- La coppia **(n, d)** = `(15, 7)` *è la **chiave privata*** ] → RSA
- Non è possibile risalire facilmente dalla chiave pubblica a quella privata (e viceversa), in quanto servirebbe conoscere il numero (p-1)(q-1), e questo implica fattorizzare n nei suoi fattori p e q (problema difficile)

`7 x 2 = 14 e 14(mod 15) = 1`

- l'inverso (mod 7) di 5 è 3 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 3 è 5 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 6 è 6 perché 6 x 6 = 36 e 36(mod 7) = 1
- l'inverso (mod 43) di 11 è 4 perché 11 x 4 = 44 e 44(mod 43) = 1

## RSA – cifratura e decifratura

Dato un messaggio m (0 < m < n) `0 < m < 33 → m = 2, c = 29`

1. Cifratura: calcolare $c = m^e \bmod n$
2. Decifratura: calcolare $m = c^d \bmod n$

Esempi:
La chiave pubblica è (33, 7) `(n, e) con e = Numero scelto a caso per trovare inverso = 2`
La chiave privata è (33, 3) `(n, d) con d = Inverso con Eulero = 14`

$c = 2^7 \bmod 33 = 29$
$m = 29^3 \bmod 33 = 2$

`m = 2, c = 2^2 mod 15 = 4 mod 15 = 4`

$c = 15^7 \bmod 33 = 27$
$m = 27^3 \bmod 33 = 15$

## RSA – generazione delle chiavi da parte di Bob

- Scegliere **due numeri primi** **p e q** p = 5, q = 7, n = p * q = 5 * 7 = 35
- Calcolare **n = pq**
- Occorre sapere **quanti sono i numeri compresi tra 1 e n che siano coprimi con n** per sceglierne uno Scegli un numero tra 1 e 35 = 4 ⟶ e
- La φ(n) di Eulero serve a tale scopo e Il risultato è **f = φ (n) = (p – 1)(q – 1) = n – p – q + 1**.
- Scegliere **e** **1 <= e < (p-1) (q-1)** *con **e** coprimo con* φ(n)
- Calcolare **d** tale che **de ≡ 1 mod (p-1) (q-1)** che sarà compreso tra 1 e φ(n)
- La coppia **(n, e)** *è la **chiave pubblica di Bob***
- La coppia **(n, d)** *è la **chiave privata di Bob***
- Non è possibile risalire facilmente dalla chiave pubblica a quella privata (e viceversa), in quanto servirebbe conoscere il numero (p-1)(q-1), e questo implica fattorizzare n nei suoi fattori p e q (problema difficile)

c = cifratura / m = decifratura (messaggio originale)

Calcolare la chiave pubblica "(n, e)" = (24, 5) → c = m^e mod n
Calcolare la chiave segreta "(n, d)" = (24, 5) → m = c^d mod n
Codificare e decodificare un messaggio m

- Mediante la **f = φ(n) di Eulero** posso sapere quanti sono i numeri compresi tra 1 e n che siano coprimi con n e ne scelgo uno che chiamo **e**
- Calcolare l'**inverso (mod f)** di **e** che identifico con **d**

Inverso = 5
5 * 5 = 25 mod 24

c = Cifratura
m = Decifratura

f = (p – 1)(q – 1) = (5 – 1) * (7 – 1) = 4 * 6 = 24
Inverso (mod 24) di 5 → 5 * 5 = 25 e (25 mod 24) = 1

ESEMPI DI INVERSO

- l'inverso (mod 7) di 5 è 3 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 3 è 5 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 6 è 6 perché 6 x 6 = 36 e 36(mod 7) = 1
- l'inverso (mod 43) di 11 è 4 perché 11 x 4 = 44 e 44(mod 43) = 1

## Algoritmo di Diffie-Hellman

g = 3, p = 5

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 $K = A^b \bmod p$

Ma:

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

SISTEMI. Compito scritto in classe sui seguenti argomenti:
Inverso di e (mod f) → RSA
Algoritmo di Diffie-Hellman
Funzione di Eulero Φ(n) → QUANTI COPRIMI / SCEGLI UNO
Calcolare la chiave pubblica
Calcolare la chiave segreta d RSA
Codificare e decodificare un messaggio m → SOPRA...

CIFRATURA DECIFRATURA