Crittografia

1. Introduzione
2. Tipi di crittografia
3. La crittografia Asimmetrica: funzionamento
4. La crittografia Asimmetrica: utilizzo
    1. cifrare i messaggi
    2. firma digitale
5. Funzioni Hash

0. Premessa

- Cosa è l'aritmetica modulare? Proviamo a renderla *easy*
  - Sono le 11:15 e se vi dico che:
    - ci vediamo tra 2 ore? 13:15
    - ci vediamo tra 24 ore? **35:15??** oppure 11:15?

In maniera implicita il vostro cervello ha ragionato in

modulo 24

ovvero ogni volta che la somma dell'orario ha raggiunto le ore 24, ricomincia a contare da 0 (in maniera ciclica!)

Il concetto di modularità (ovvero *resto della divisione intera*) sarà FONDAMENTALE per la crittografia e per comprenderne il suo funzionamento

Qualche esempio:

- 5 mod 3 = 2 perchè 5:3=1 con il resto di 2
- 25 mod 5 = 0 perchè 25:5=5 con il resto di 0
- 50 mod 30 = ___ perché 50:30 = ___ con il resto di ____

In sintesi **X mod Y = n** tenendo presente che SEMPRE **n < Y**

La relazione di congruenza si ha quando in MOD i valori sono equivalenti,

ad es. *15≡30≡155≡0 mod 5*

1. Introduzione

- La **crittografia** è la disciplina che studia le tecniche per proteggere la ***riservatezza***, l'***integrità*** e l'***autenticità*** delle informazioni attraverso la trasformazione dei dati in un formato illeggibile per chi non possiede le chiavi appropriate per decifrarli...

... in tempo utile!

Quindi consente di *codificare* un messaggio in modo che solo il destinatario autorizzato possa leggerlo, utilizzando algoritmi matematici e chiavi segrete.

2. Tipi di crittografia

- La **crittografia** si distingue, a seconda delle chiavi utilizzate per cifrare il dato, in:
  - SIMMETRICA: la chiave usata per cifrare e quella per decifrare è la stessa (a patto di cambi di operazione).
    - *Esempio*: il cifrario di cesare - si veda il gadget-regalo
  - ASIMMETRICA: la chiave usata per cifrare non è la stessa utilizzata per decifrare, nononstante le due chiavi siano "connesse tra loro" (sono una coppia di chiavi)
    - *Esempio*: lo vediamo ora!

3. Crittografia Asimmetrica: funzionamento

- **Principio base**
  - Una chiave cifra, l'altra decifra
  - Chiave pubblica vs chiave privata
- **Esempio pratico**
  - Alice vuole mandare un messaggio sicuro a Bob usando la chiave pubblica di Bob
  - Solo Bob potrà decifrarlo con la sua chiave privata

3. Crittografia Asimmetrica: funzionamento

- **In pratica, quindi?**
  - Bob genera una coppia di chiavi, una **pubblica** e una **privata**
  - Bob rende disponibile (su un sito di condivisione conosciuto da tutti) la sua chiave **pubblica**
  - Alice vuole mandare un messaggio a Bob
  - Alice compone il messaggio e lo cifra con la chiave **pubblica** di Bob
  - Alice invia il messaggio a Bob
  - Solo Bob potrà decifrare il contenuto del messaggio, perchè lui solo possiede la chiave accoppiata a quella pubblica usata da Alice, ovvero la sua (di Bob) chiave **privata**.

Quindi non ci importa nulla se qualcuno viene a conoscenza del messaggio che Alice sta inviando a Bob perchè esso è cifrato e solamente Bob ha modo di decifrarlo!

3. Crittografia Asimmetrica: utilizzo

- **In pratica, quindi?**
  - Bob genera una coppia di chiavi, una **pubblica** e una **privata**
  - Bob rende disponibile (su un sito di condivisione conosciuto da tutti) la sua chiave **pubblica**
  - Alice vuole mandare un messaggio a Bob
  - Alice compone il messaggio e lo cifra con la chiave **pubblica** di Bob
  - Alice invia il messaggio a Bob
  - Solo Bob potrà decifrare il contenuto del messaggio, perchè lui solo possiede la chiave accoppiata a quella pubblica usata da Alice, ovvero la sua (di bob) chiave **privata**

3. Crittografia Asimmetrica: utilizzo pratico

1. **Cifrare i messaggi - CONFIDENZIALITÀ del messaggio**
   - Domandina pratica: come creo le chiavi (privata **q** e pubblica **p**)?
   - trovo due *numeri primi* **p** e **q**. Ad es: p = 61 q = 53
     e ottengo N = p * q (sarà il **modulo**) ovvero **3233**
     scelgo un numero primo **e** = 17 (chiave pubblica) e per calcolare la sua rispettiva privata, calcolo **d** ≡ e^{-1} mod φ(N), in questo caso 2753 sarà la chiave privata.
   - Bob genera le chiavi e pubblica **e** come alla slide precedente.
   - Alice vuole comunicare il pin 1234 quindi critta eseguendo 1234^{17} mod **3233** (ovvero **2548**) e invia
   - Bob riceve il messaggio e per decifrarlo calcolerà $\mathbf{2548}^{2753}$ mod 3233. Indovinate quanto fa? _____

3. Crittografia Asimmetrica: utilizzo pratico

2. **Firma Digitale - AUTENTICITÀ DEL MESSAGGIO**

- Vi ricordate la slide precedente?
- Ecco Bob ha sempre generato due chiavi ma questa volta critta il messaggio con la sua chiave privata
- Con i passaggi spiegati prima, chiunque con la chiave pubblica può verificare che quel messaggio sia veramente di BOB perchè solo lui poteva crittare con la chiave privata corrispondente!
- Ma in realtà BOB per certificare il suo messaggio non critta tutto il messaggio con la sua chiave privata, è infatti una operazione molto onerosa computazionalmente!
- Quindi BOB cosa critta? l'HASH del messaggio!

4. Funzioni HASH

- **Cosa sono le funzioni hash?**
  - Trasformano dati in una *impronta digitale* univoca
  - Esempi: SHA-256, MD5
- **Proprietà fondamentali**
  - Unicità: due input diversi devono produrre hash diversi
  - Irreversibilità: impossibile risalire al dato originale
  - Sensibilità ai cambiamenti: piccole modifiche generano hash completamente diversi
  - Produce sempre un output di dimensione fissata

4. Funzioni HASH

Qualche esempio

- **PROPRIETÀ DI LUNGHEZZA FISSATA IN OUTPUT**
  - `"Ciao" -->  16272a5dd83c63010e9f67977940e871`
  - `"Ciao mamma" ->  195a187d3a09bafbf879c5cd2a21cadf`
- **PROPRIETÀ DI SENSIBILITÀ DI INPUT**
  - **Esempio banale**
    - `"Ciao" ->  16272a5dd83c63010e9f67977940e871`
    - `"Ciap" ->  e7e323dbf9b71073c293216a75366492`
  - **Esempio un po' più articolato**
    - `"Nel mezzo del cammin di nostra vita mi ritrovai per una selva"`
      `10bdca48db44daff4ec775d694f65d22`
    - `"Nel mezzo del cammin di nostra vita mi ritrovai per una solva"`
      `83622f0c126821eab2ad3e31873ff8ae`

Apprezziamo meglio questa ultima proprietà se confrontiamo i cambiamenti di una sola lettera cifrando con il cifrario di Leon Battista Alberti