**Lez2 13/11/2024**

**Intro Crittografia (consulta presentaizone)**

storia tecniche ecc

Alice -> msg C -> Bob | Eve intercetta e viene impedito con crittografia

function(Msg) = Code

crittografia sempre applicata storicamente

4500 anni fa ca

comparsa nel VI sec aC

**cifrari monoalfabetici:** algoritmo che rende msg in code o viceversa attraverso determinati passaggi

codice = significato

cifrario = singolo carattere

***Esempi storici***

*cifrario di atbash:* alfabeto normale, lettere corrispondono inversione alfabeto

*steganografia:* contenutomessaggio nascosto (principio da cui deriva il watermarking)

NB: la crittografia protegge il contenuto rendendolo illeggibile, la cosa necessaria per lettura, ma nascosta, è la chiave per poter leggere (***principio di kerchoff***)

function(Msg, Key) = Content

*cifrario di cesare:* chiave shift, si usa carattere spostato, debole ai giorni nostri inutile

soluzione permutazione “casuale” delle lettere alfabeto, no ripetizione ma sono sempre 26 caratteri

nei cifrari monoalfabetici la chiave è il mescolamento essenzialmente, violabile dai

**tipi di attacchi.**

forza bruta: tentativi

statistico: sfrutta ripetizioni carattere

**cifrari polialfabetici:** algoritmo che fa uso di + alfabeti, quindi + regole (cioé chiave) stabilite, per crittografare il msg

***Esempi storici***

*cerchio alberti:* 2 dischi, chiave(char disco 1 corrisponde char disco 2), il msg veniva criptato anche con + chiavi (+resistenza a attacco statistico)

*cifrario di* vigenère:chiave(parola segreta), rimossi spazi applico chiave fino alla fine del msg

**Crittoanalisi**

metodo con cui si decifrò il cifrario di vigenere

affrontare

ripetizioni di porzioni di codice

conosco la chiave (lunghezza)