Laboratorio di crittografia

Piano Lauree Scientifiche

Collaborazione

Dipartimento di Matematica

ITIS Leonardo da Vinci

Partecipanti

- Docenti
  - Università
    - Alessandro Zaccagnini
  - ITIS
    - Alessandra Melej
    - Alberto Ferrari
  - Studenti Laurea Magistrale
    - Luigi Corvacchiola
    - Giovanna Di Donna
- Studenti
  - Conciatori
  - Curati Emanule
  - La Porta Alfonso
  - N'Dyaie Lamine
  - Paini
  - Pessina Matteo
  - Savic Jonathan
  - Valenti Andrea

Argomenti trattati negli incontri

- Introduzione alla crittografia
- Presentazione del linguaggio di scripting PARI/GP
- Crittografia classica
- Crittografia moderna

- Gli incontri si sono svolti nei laboratori dell'ITIS Leonardo da Vinci

I due gruppi

Crittografia

- Occultamento del significato del messaggio
- Comunicazione segreta

Crittoanalisi

- Interpretazione del messaggio ignorando la chiave utilizzata per crittare il messaggio

Hacker: white hat («i buoni»)

- Un white hat (letteralmente "cappello bianco"), chiamato anche **hacker etico**, è un hacker che si oppone all'abuso dei sistemi informatici. La sua attività è di verifica della sicurezza di una rete e dei sistemi che la compongono, per individuare il livello di rischio cui sono esposti i dati, e proporre eventuali azioni correttive per migliorare il grado di sicurezza.

Hacker: black hat («i cattivi»)

- Un black hat (**cracker**) è un hacker **malintenzionato** o con intenti criminali. Questo termine è spesso utilizzato nel campo della sicurezza informatica e dai programmatori per indicare una persona dalle grandi capacità informatiche, ma con fini illeciti.

Crittografia

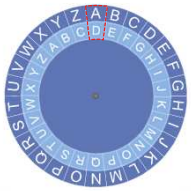
- Il **messaggio in chiaro** viene "offuscato" in modo da non essere comprensibile a persone non autorizzate tramite un **algoritmo di crittografia** che utilizza una **chiave** (*Ke* chiave di crittazione).
- Il **messaggio crittato** ricevuto dal destinatario viene decrittato mediante lo stesso algoritmo utilizzando la **chiave di decrittazione** (*Kd*).

Il metodo di Cesare

- Il cifrario di Cesare è un cifrario a sostituzione **monoalfabetica**
  - ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni successive nell'alfabeto.
- La sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.
- Un esempio con chiave 3:

PIANO LAUREE SCIENTIFICHE
SLDQR ODXUHH VFLHQWLILFKH

Cifrari a scorrimento



La nostra applicazione Java

Cesare: crittare un carattere

```
// parametri: carattere e chiave di codifica
public char criptaCar (char c, int ke){
  int app;
  if(tonum(c)!=-1){ //carattere dell'alfabeto
    app=tonum(c);   //converto in numero
    // crittazione mediante aggiunta della chiave
    // addizione modulo n (dimensione alfabeto)
    app=modulo(app+ke,alpha.length());
    return tochar(app);//riconversione in carattere
  }
  // se non fa parte dell'alfabeto ritorna inalterato
  return c;
}
```

Cesare: decrittare un carattere

- La **chiave di decrittazione** si ottiene facilmente dalla chiave utilizzata per crittare il messaggio.
- Kd = Mod(N-Ke)
- Dove N è la dimensione dell'alfabeto utilizzato (nei nostri esempi 26)
- La procedura di decrittazione risulta quindi identica a quella di crittazione

Black hat e metodo di Cesare

- Nel nostro esempio simuliamo l'intercettazione del messaggio crittato e il tentativo di ottenere il messaggio in chiaro **senza conoscere la chiave**.
- Utilizziamo due metodi:
  - Brute force
    - Tentativi utilizzando ognuna delle possibili chiavi
    - Possibile dato il numero limitato di chiavi (N-1)
  - Analisi di frequenza
    - Individuare il carattere più frequente del testo crittato e confrontarlo con quello più frequente nella lingua utilizzata per la comunicazione.

Brute force

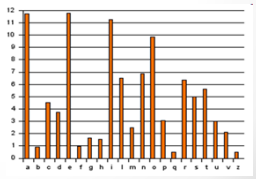
- Forza bruta: consiste nel verificare tutte le soluzioni teoricamente possibili fino a che si trova quella effettivamente corretta.
- Un esempio pratico di attacco di forza bruta è quello tentare di aprire una valigetta con serratura a combinazione provando tutte le possibili combinazioni delle rotelle numerate.

Analisi di frequenza

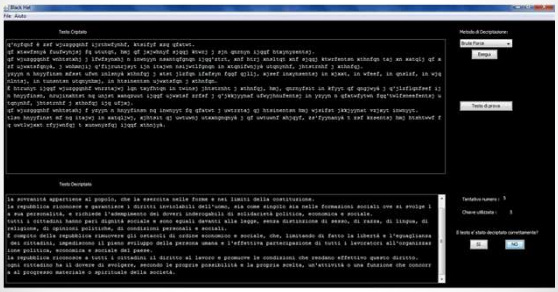
- In ogni lingua la frequenza di uso di ogni lettera è piuttosto determinata. Una volta trovata la lettere più frequente nel testo criptato si prova a sostituire con le lettere più frequenti.

Le lettere più frequenti:

Italiano		Inglese	
E	11,79 %	E	12,31 %
A	11,74 %	T	9,59 %
I	11,28 %	A	8,05 %
O	9,83 %	O	7,94 %
N	6,88 %	N	7,19 %



La nostra applicazione Java



Il cifrario di Vigenère

- E' il più semplice dei cifrari polialfabetici.
- Fu **ritenuto per secoli inattaccabile**.
- Si può considerare una generalizzazione del cifrario di Cesare: invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto, determinato in base ad una parola chiave da scrivere ripetutamente sotto il messaggio, carattere per carattere.
- Un esempio:
  - `PIANO LAUREE SCIENTIFICHE`
  - `ITISITISITISITISITISITISI`
  - `XBIFW EIMZXM KKBMFBBNAKAM`

Debolezza del metodo di Vigenère

- Questo metodo è stato considerato sicuro per alcuni secoli, finche un'analisi statistica più raffinata, di Kasinski, mostrò che è possibile "indovinare" la lunghezza k della chiave di cifratura, riducendo il problema della decifratura a k problemi di decifratura del metodo di Cesare.
- L'analisi si basa sul fatto che in ogni lingua vi sono alcune combinazioni di due lettere piuttosto frequenti: se due istanze di questa coppia di lettere compaiono nel testo in chiaro ad una distanza che è un multiplo della lunghezza della chiave, saranno cifrate allo stesso modo, perché vanno a finire nelle stesse colonne.

Cryptographia ad usum Delphini – A. Zaccagnini

Debolezze

- La debolezza comune ai metodi presentati è la **necessità di scambio della chiave** fra mittente e destinatario.
- Intercettare la comunicazione in cui viene inviata la chiave permette poi di decifrare tutti i messaggi.