Registri a scorrimento e cifrari a flusso

Daniele Argento
Riaz Bashir
Davide Capomagi
Roberto Manicardi

I cifrari a flusso

- alfabeto di q simboli qualsiasi $\{a_1, a_2, \ldots, a_q\}$
- quadrato latino di ordine q
- chiave lunga almeno quanto il messaggio in chiaro

Messaggio in chiaro $m = m_1 m_2 \ldots m_n$
Chiave $k = k_1 k_2 \ldots k_n$
Ottengo il **cifrato** c_i in questa maniera:

$$c_i = m_i \oplus k_i$$

Tipi di sicurezza

- **Sicurezza assoluta**: un cifrario è **assolutamente sicuro** se l'incertezza a priori sul testo in chiaro è uguale all'incertezza a posteriori (cioè dopo aver analizzato in ogni modo possibile il testo cifrato)

- **Sicurezza computazionale**: un cifrario è **computazionalmente sicuro** se calcolare m da c, senza conoscere k, richiede una potenza di elaborazione superiore a quella a disposizione del crittoanalista

One-Time-Pad

Inventato da Vernam nel 1917 come sistema di protezione crittografica per comunicazioni su telegrafo.

- testi codificati in **binario**
- cifrario a flusso **simmetrico**
- chiavi **monouso** e **generate casualmente**
- funzione di cifratura basata su $\oplus \ mod \ 2$
- XOR bit a bit sui computer

Sicurezza del One-Time-Pad

Se la chiave è realmente casuale, il one-time-pad è perfettamente sicuro contro crittoanalisi basata soltanto sul testo cifrato.

- impossibilità di decrittare il cifrato senza la chiave
- **inutilità di una ricerca brute force nello spazio delle chiavi**
- **tutti i possibili testi in chiaro sono decrittazioni equiprobabili del cifrato**

Gestione delle chiavi

Problemi:
- chiavi molto lunghe $\Rightarrow$ **costi molto elevati**
- chiavi non casuali $\Rightarrow$ **dipendenza statistica**

- necessità di generare una chiave **pseudocasuale** a partire da una quantità di dati iniziali breve

- sequenza casuale regolata da una certa funzione di un parametro iniziale

- la funzione e il parametro costituiscono la nuova **chiave segreta**

Sequenze pseudocasuali

- numero **arbitrario**: un numero qualunque

- numero **casuale**: un numero estratto da un insieme finito di valori equiprobabili

I numeri casuali generati da un computer vengono detti **pseudocasuali**.

Requisiti di una sequenza casuale:
- periodo lungo
- ordinamento interno non uniforme
- sequenze non correlate
- uniformità nell'emissione dei valori

Metodo Middle Square

Ideato da Von Neumann nel 1946, è il primo algoritmo per la generazione di sequenze di numeri casuali:

1. scelgo a_0 come **base** della sequenza

2. calcolo il valore n-esimo della sequenza:
   $a_{n+1} = m$ cifre intermedie di $(a_n)^2$

Suppongo che a_n^2 ha k cifre: le m cifre intermedie di a_n^2 vanno dalla $(k+m)/2$-esima alla $(k-m)/2$-esima

Esempio di generazione

- Parametri iniziali a_0=1422, m = 3

$a_0^2 = 2\ 0\ 2\ 2\ 0\ 8\ 4 \Rightarrow k = 7$

Range cifre intermedie: dalla 2 alla 5 $\Rightarrow a_1 = 2\ 2\ 0\ 8$

La sequenza parziale è: 1 4 2 2 2 2 0 8

Problemi:
- si presentano spesso cicli brevi di elementi
- la sequenza può decrescere fino a zero

Generatore lineare congruenziale

Ideato da Lehmer nel 1951 è ancora oggi il metodo più usato. Si basa sulla formula seguente:

$$X_n = (aX_{n-1} + c) \ mod \ m$$

- Successione definita per ricorrenza
- Insieme dei valori finito $[0, m-1]$

$\Rightarrow$ **successione periodica**

Scelta dei parametri

- inizializzazione di X_0
- generazione al massimo di m valori distinti

$\Rightarrow$ **m dev'essere scelto abbastanza grande**

- generare sequenze di periodo massimo

Esempio di generazione

- Parametri iniziali: $X_0 = 3, m = 9, c = 2, a = 7$

$$X_1 = (7 * 3 + 2) \ mod \ 9 = 5$$
$$X_2 = (7 * 5 + 2) \ mod \ 9 = 1$$
$$X_3 = (7 * 1 + 2) \ mod \ 9 = 0$$
$$X_4 = (7 * 0 + 2) \ mod \ 9 = 2$$
$$X_5 = (7 * 2 + 2) \ mod \ 9 = 7$$
$$X_6 = (7 * 7 + 2) \ mod \ 9 = 6$$
$$X_7 = (7 * 6 + 2) \ mod \ 9 = 8$$
$$X_8 = (7 * 8 + 2) \ mod \ 9 = 4$$
$$X_9 = (7 * 4 + 2) \ mod \ 9 = 3$$
$$X_{10} = (7 * 3 + 2) \ mod \ 9 = 5$$

Metodo della congruenza quadratica

Ideato da Knuth nel 1981. Si basa su una successione definita per ricorrenza:

$$X_n = (aX_{n-1}^2 + bX_{n-1} + c) \ mod \ m$$

Esempio di generazione

Parametri iniziali: a=2, b=3, c=1, m=4

$X_1 = (2 * 4 + 3 * 2 + 1) \ mod \ 4 = 3$
$X_2 = (2 * 9 + 3 * 3 + 1) \ mod \ 4 = 0$
$X_3 = (2 * 16 + 3 * 4 + 1) \ mod \ 4 = 1$
$X_4 = (2 * 1 + 3 * 1 + 1) \ mod \ 4 = 2$
$X_5 = (2 * 4 + 3 * 2 + 1) \ mod \ 4 = 3$