CRITTOGRAFIA A.A. 2025-26 FOGLIO ESERCIZI 3

Mandare gli a guidomaria.lido@gmail.com o consegnarli a lezione entro venerdì 12 dicembre. Se via mail, consegnare gli esercizi un file PDF facilmente stampabile e scrivere nome e cognome nel file PDF (non solo nel nome). Se possibile scrivere il codice anche nel file (non mi aspetto aspetto sia lunghissimo)

È ammesso scambiare idee ma ognuno deve scrivere le soluzioni in autonomia.

Risolvere due esercizi tra gli esercizi $7.1, \dots, 7.6$ dello Stinson paterson e uno degli esercizi seguenti.

1) *Birthday "paradox" con probabilità qualsiasi* Dimostrare se Ω è un insime di N elementi dotato di una probabilità possibilimente non uniforme, allora dopo $3\lceil\sqrt{N}\rceil$ estrazioni indipendenti di elementi da Ω, la probabilità di aver estratto elementi tutti diversi è minore di $1/2$.

2) *(Euristica vista a lezione sull'efficacia del metodo rho di Pollard)*

   Sia G un gruppo ciclico di ordine primo N. Sia g un suo generatore, sia h un elemento diverso dall'elemento neutro e denotiamo $\pi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to G$ la mappa $\pi(a,b) = g^a h^b$. Scegliamo $(a_0, b_0, x_0 = g^{a_0}h^{b_0})$ in $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \times G$.

   Sia $f\colon G \to G$ una funzione casuale e $\tilde{f}\colon (\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$ una funzione casuale tra quelle tali che $\pi(\tilde{f}(a,b)) = f(\pi(a,b))$ per ogni $(a,b) \in (\mathbb{Z}/N\mathbb{Z})^2$. Allora possiamo alcolare la successione per ricorrenza (a_i, b_i, x_i) con $(a_i, b_i) = \tilde{f}(a_{i-1}, b_{i-1})$ e $x_i = \tilde{f}(x_{i-1})$.

   Dimostrare che con probabilità maggiore di una costante si trova un indice $i < 3\lceil\sqrt{N}\rceil$ tale che $x_i = x_{2i}$ ma $b_i \neq b_{2i}$.

3) Data una hash function H a valori in un insieme di N elementi, descrivere un algoritmo probabilistico che trovi collisioni di H con in media $\sqrt{N}$ operazioni, ma che usi memoria costante. É preferibile che l'algoritmo dipenda da un parametro che introduca della "randomicità", cosicchè, fissata una hash H, esistano più possibili modi di attaccarla e si possa sperare almeno un attacco funzioni.