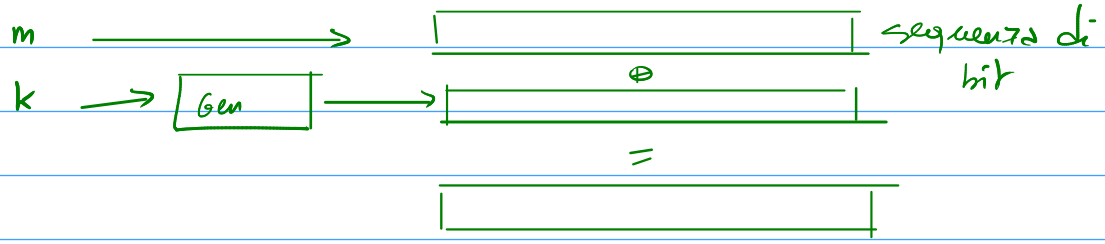
Stato → STREAM CYPHER



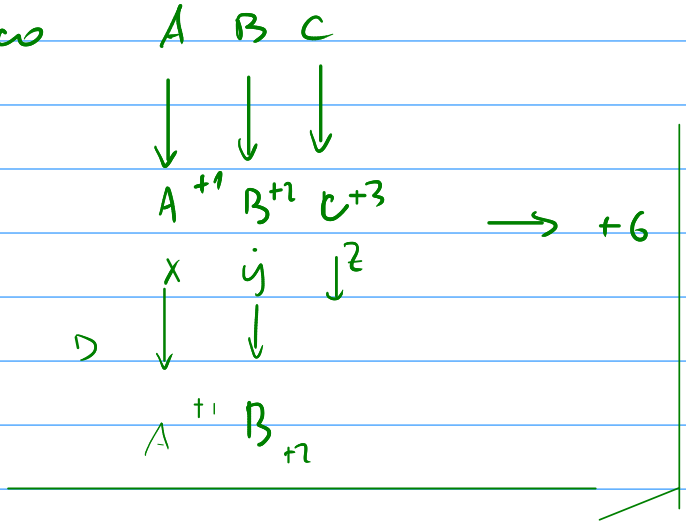

N.B chosen plaintext → noi offriamo parte della sequenza → cerchiamo di ricavare la chiave k oppure lo stato interno del generatore.

i) → DEVE ESSERE DIFFICILE DATO L'OUTPUT DI "Gen" ricostruire il suo stato interno

ii) → DEVE essere difficile dati t bits in output da "Gen" indovinare il bit (t+1)-esimo

↑ RC4 → Wep

codifico A B C




pb fondamentale in tutti i casi considerati

→ DISTRIBUZIONE DELLE CHIAVI

→ OTTIMALE → negoziare una chiave esattamente quando serve

ed usarla una e una sola volta.

PFS = Perfect Forward Secrecy → Se anche una chiave è scoperta dall'avversario questo fornisce informazioni solamente per il messaggio per cui è stata usata.

Diffie-Hellman (DH) di scambio di chiavi

Sia $G = \langle g \rangle$ gruppo ciclico generato da $g$

| ALICE | BOB. |
|---|---|
| $a \in \mathbb{N}$ NONCE | $\beta \in \mathbb{N}$ NONCE |
| $a = g^a$ | $b = g^\beta$ |
| $\longrightarrow a$ | |
| $b \longleftarrow$ | |
| $k = b^a = g^{\beta a} = g^{a\beta}$ | $k = a^\beta = g^{a\beta}$ |

Se Eve da $a$ sa ricavare $a \Rightarrow$
Eve calcola $b^a$ come ALICE e trova $k$

questo è il problema del DLOG = Logaritmo Discreto.
→ supponiamo non risolvibile.