Esercizi di Crittografia

11 gennaio 2023

Nota. La codifica usata per i plaintext è:

`"␣" = 0, "a" = 1, "b" = 2, ..., "z" = 26`

0x0

I cifrari alla cui base c'è una relazione lineare non sono molto robusti. *Si pensi a come si dice collina in inglese.*

0x1

RSA è un cifrario robusto se usato correttamente. Alle volte però bisognerebbe stare attenti alle relazioni tra gli esponenti pubblici...

0x2

In RSA si può essere esposti anche quando la scelta dell'esponente non è felice. Questo rappresenta una debolezza intrinseca, ad esempio, quando è troppo basso oppure...

0x3

Domanda: quale curva ellittica usereste per cifrare tra le due proposte? Perché? Si riescono a recuperare i testi in chiaro? Per questo esercizio si usi il seguente protocollo.

1. Si sceglie una curva ellittica sul campo $\mathbb{F}_p$ con equazione $y^2 = x^3 + Ax + B$ e un generatore G (un punto della curva).
2. Alice sceglie una chiave privata n la cui corrispondente chiave pubblica è $Q = nG$.
3. Bob sceglie un testo in chiaro M e un k random. Calcola $P = kG$ e $C = M + kQ$. Manda (P, C) ad Alice.
4. Alice calcola $C - nP$ e legge M.