CR1 – Crittografia 1

Alfonso Pesiri - Fabrizio Zaccari

Tutorato 3 – 19 Marzo 2008

Esercizio 1. Calcolare i seguenti inversi moltiplicativi:

$$7^* \bmod 120,\ 3^* \bmod 331,\ 7^* \bmod 352.$$

Esercizio 2. Si consideri il sistema RSA con chiave pubblica $(n,\, e) = (143,\, 37)$.

1. Cifrare il messaggio $M = 56$. Ovvero, calcolare il resto, che si denoterà con $\bar{M}$, della divisione per 143 del numero 56^{37}.

2. Decifrare il messaggio $\bar{M}$. Ovvero, calcolare l'esponente segreto d tale che $\bar{M}^d \equiv M \bmod 143$.

Esercizio 3. Consideriamo un alfabeto binario $\{0,\, 1\}$ e un sistema che invia pacchetti fissi di 6 bit. Dopo aver fissato i parametri RSA coerentemente con i dati iniziali, ed aver indicato la chiave pubblica e quella privata, spedire il seguente messaggio:

$$10111010101$$

Una volta fattorizzato il modulo RSA, indicare un possibile attaco al crittosistema.

Esercizio 4. In un sistema RSA la chiave pubblica è $(n,\, e) = (6089561,\, 125)$. Sapendo che la differenza tra i due primi che costituiscono il modulo RSA è 160, calcolare l'esponente di cifratura d.

Esercizio 5. Un utente deve scegliere la propria chiave RSA secondo i seguenti principi:

1. l'alfabeto utilizzato ha 7 caratteri: $\{a,\, e,\, i,\, o,\, u,\, x,\, y\}$;
2. il sistema permette di inviare pacchetti con al più 3 caratteri;
3. la chiave pubblica può essere scelta liberamente.

Dopo aver generato una chiave pubblica RSA e la corrispondente chiave privata, inviare il messaggio

$$xaeayo$$