CR1 – Crittografia 1

Alfonso Pesiri - Fabrizio Zaccari

Tutorato 4 – 3 Aprile 2008

Esercizio 1. Calcolare i seguenti simboli di Jacobi:

1. $\left(\frac{12321}{55555}\right)$;
2. $\left(\frac{234564}{134431}\right)$;
3. $\left(\frac{983932}{72637}\right)$.

Esercizio 2. Sapendo che $m \equiv 3 \bmod 4$, $m \equiv 2 \bmod n$, $n \equiv 1 \bmod 8$, calcolare il seguente simbolo di Jacobi: $\left(\frac{(5m+n)^3}{m}\right)$.

Esercizio 3. Calcolare $5^{13340} \bmod 143$. *Non usare la calcolatrice!*

Esercizio 4. Si consideri l'alfabeto composto dai caratteri: $\{-,\ o,\ l,\ n,\ s\}$. Sapendo che la lunghezza dei pacchetti è di tre caratteri, decifrare il messaggio

$$-onnlnnsn\,.$$

Si utilizzino i seguenti dati: $n = 187$, $p - q = 6$, $e = 7$.

Esercizio 5. Un intero composto n si dice *numero di Carmicheal* se

$$a^{n-1} \equiv 1 \bmod n$$

per ogni a coprimo con n.

1. Dimostrare che 8911 è un numero di Carmicheal.
2. Dimostrare che se n è di Carmicheal, allora n ha almeno tre fattori primi.

Esercizio 6. Applicare il test di Solovay – Strassen ai seguenti interi, considerando le basi a indicate.

1. $n = 77$, $a = 43,\ 76$;
2. $n = 73$, $a = 5,\ 11$.

Cosa possiamo concludere circa la primalità di n?