CR1 – Crittografia 1

Alfonso Pesiri - Fabrizio Zaccari

Tutorato 5 – 24 Aprile 2008

Esercizio 1. Utilizzando il metodo di fattorizzazione alla Fermat, trovare almeno un fattore proprio dei seguenti interi:

1. $n = 2527$;
2. $n = 9797$;
3. $n = 142763$.

Esercizio 2. Utilizzando il metodo di fattorizzazione Rho di Pollard, fattorizzare i seguenti interi:

1. $n = 731$;
2. $n = 943$;
3. $n = 3013$.

Esercizio 3. Fattorizzare l'intero $n = 667$ utilizzando il metodo $p - 1$ di Pollard. *Suggerimento:* $n = pq$, *ove* $p - 1$ *è* B*–liscio, con* $B = 11$.

Esercizio 4. Sia $n = pq = 1060459$ un modulo RSA, di cui è noto che la distanza tra i due primi p e q è piccola. Mostrare come è possibile attaccare il sistema.

Esercizio 5. Applicare il test di Solovay – Strassen all'intero 123, utilizzando come prima base $a = 5$ e nell'ordine, se necessario, le basi $2, 3, 6, 7$. Cosa si può concludere?

Esercizio 6. Applicare il test di Poklington all'intero $n = 503$, dimostrando che esso è primo.