CR1 – Crittografia 1

Alfonso Pesiri - Fabrizio Zaccari

Tutorato 2 – 13 Marzo 2008

Esercizio 1. Utilizzando il Piccolo Teorema di Fermat dimostrare che:

1. $n^2 - n$ è multiplo di 2;
2. $n^3 - n$ è multiplo di 6;
3. $n^5 - n$ è multiplo di 30;
4. $n^7 - n$ è sempre divisibile per 42.

Esercizio 2. Dato il numero binario $n = (111011001010)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive.

Esercizio 3. Utilizzando il metodo dei quadrati successivi calcolare:

1. $3^{10} \mod 8$;
2. $3^{26} \mod 17$;
3. $2^{300} \mod 23$.

Esercizio 4.

Utilizzando prima l'algoritmo euclideo delle divisioni successive e poi l'algoritmo binario calcolare:

$$\mathrm{MCD}(7, 352),\ \mathrm{MCD}(105, 418),\ \mathrm{MCD}(1144, 1463).$$

e trovare un'identità di Bézout.

Esercizio 5. Fattorizzare completamente il numero $5^{24} - 1$.