RACCOLTA DI ALCUNI ESERCIZI TRATTI DA COMPITI D'ESAME SUL SISTEMA CRITTOGRAFICO RSA

Attenzione: questi sono alcuni esercizi d'esame, sugli argomenti di questa dispensa. Non sono una selezione di quelli che ritengo più significativi, ma solamente quelli tratti daglia appelli di cui sono in possesso del file sorgente. Siete quindi invitati a cercare di risolvere gli esercizi, su questi argomenti, tratti dai TUTTI gli esami degli anni passati (oltre agli esercizi assegati, naturalmente).

Esercizio 0.1. Si consideri il sistema crittografico RSA corrispondente al modulo $n = 143 = 11 \cdot 13$ e all'esponente $D = 53$.

(a) Cifrare il messaggio "24", cioè calcolare il resto della divisione per 143 del numero 24^{53} (suggerimento: calcolare il resto delle divisioni per 11 e per 13 del numero 24^{53});

(b) Determinare un esponente E che consente di decifrare il messaggio precedente. In altre parole: determinare un numero naturale E tale che $(24^{53})^E \equiv 24 \pmod{143}$. (a) Siccome $53 \equiv$

$3 \pmod{10}$, abbiamo per il Teorema di Fermat che $x = 24^{53} \equiv 2^3 \equiv 8 \pmod{11}$. Similmente, $53 \equiv 5 \pmod{12}$ e quindi $x = 24^{53} \equiv (-2)^5 \equiv -32 \equiv 7 \pmod{13}$. Con il Teorema Cinese del resto si trova che $x \equiv 85 \pmod{143}$. (b) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 53 \equiv 1 \pmod{10 \cdot 12}$ va bene. Per trovare una soluzione, si applica l'algoritmo Euclideo:

$$1 \cdot 120 + 0 \cdot 53 = 120,$$
$$0 \cdot 120 + 1 \cdot 53 = 53,$$
$$1 \cdot 120 - 2 \cdot 53 = 14,$$
$$-3 \cdot 120 + 7 \cdot 53 = 11,$$
$$4 \cdot 120 - 9 \cdot 53 = 3,$$
$$-15 \cdot 120 + 34 \cdot 53 = 2,$$
$$19 \cdot 120 - 43 \cdot 53 = 1.$$

L'esponente cercato è quindi $E = -43 + 120 = 77$.

Esercizio 0.2. Usando il sistema RSA, si supponga che il modulo dell'utente sia $n = 7 \cdot 11$ e che l'esponente pubblico sia $D = 29$. Determinare l'esponente segreto E che consente di decifrare i messaggi. In altre parole, determinare un numero naturale E tale che $(a^D)^E \equiv a \pmod{n}$ per ogni a tale che $\mathrm{mcd}(a, n) = 1$.

(a) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 29 \equiv 1 \pmod{6 \cdot 10}$ va bene. Per trovare una soluzione, si applica l'algoritmo Euclideo:

$$1 \cdot 60 + 0 \cdot 29 = 60,$$
$$0 \cdot 60 + 1 \cdot 29 = 29,$$
$$1 \cdot 60 - 2 \cdot 29 = 2,$$
$$-14 \cdot 60 + 29 \cdot 29 = 1.$$

L'esponente cercato è quindi $E = 29$.

Esercizio 0.3. Si consideri il sistema crittografico RSA corrispondente al modulo $n = 143 = 11 \cdot 13$ e all'esponente $D = 53$.

(a) Cifrare il messaggio "24", cioè calcolare il resto della divisione per 143 del numero 24^{53} (suggerimento: calcolare il resto delle divisioni per 11 e per 13 del numero 24^{53});

(b) Determinare un esponente E che consente di decifrare il messaggio precedente. In altre parole: determinare un numero naturale E tale che $(24^{53})^E \equiv 24 \pmod{143}$.

(a) Siccome $53 \equiv 3 \pmod{10}$, abbiamo per il Teorema di Fermat che $x = 24^{53} \equiv 2^3 \equiv 8 \pmod{11}$. Similmente, $53 \equiv 5 \pmod{12}$ e quindi $x = 24^{53} \equiv (-2)^5 \equiv -32 \equiv 7 \pmod{13}$. Con il Teorema Cinese del resto si trova che $x \equiv 85 \pmod{143}$. (b) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 53 \equiv 1 \pmod{10 \cdot 12}$ va bene. Per trovare una soluzione, si applica l'algoritmo Euclideo:

$$\begin{aligned}
1 \cdot 120 + \ 0 \cdot 53 &= 120,\\
0 \cdot 120 + \ 1 \cdot 53 &= 53,\\
1 \cdot 120 - \ 2 \cdot 53 &= 14,\\
-3 \cdot 120 + \ 7 \cdot 53 &= 11,\\
4 \cdot 120 - \ 9 \cdot 53 &= 3,\\
-15 \cdot 120 + 34 \cdot 53 &= 2,\\
19 \cdot 120 - 43 \cdot 53 &= 1.
\end{aligned}$$

L'esponente cercato è quindi $E = -43 + 120 = 77$.

Esercizio 0.4. Si consideri il sistema crittografico RSA corrispondente al modulo $n = 143 = 11 \cdot 13$ e all'esponente $D = 47$.

(a) Cifrare il messaggio "17", cioè calcolare il resto della divisione per 143 del numero 17^{47} (suggerimento: calcolare il resto delle divisioni per 11 e per 13 del numero 17^{47});

(b) Determinare un esponente E che consenta di decifrare il messaggio precedente. In altre parole: determinare un numero naturale E tale che $(17^{47})^E \equiv 17 \pmod{143}$.

(a) Siccome $47 \equiv 7 \pmod{10}$, abbiamo, per il Teorema di Fermat, che $x = 17^{47} \equiv 6^7 = 36^3 \cdot 6 \equiv 3^3 \cdot 6 = 27 \cdot 6 \equiv 5 \cdot 6 \equiv 8 \pmod{11}$. Similmente, $47 \equiv -1 \pmod{12}$ e quindi $x = 17^{47} \equiv 4^{-1} \pmod{13}$. Usando l'algoritmo euclideo si calcola che l'inverso moltiplicativo di 4 (mod 13) è uguale a 10. Abbiamo quindi che $17^{47} \equiv 10 \pmod{13}$. Con il Teorema Cinese del resto si trova che $x \equiv 140 \pmod{143}$.

(b) Ogni soluzione $E \in \mathbf{N}$ della congruenza $E \cdot 47 \equiv 1 \pmod{10 \cdot 12}$ fornisce un possibile esponente. Per trovare una soluzione, si applica l'algoritmo Euclideo:

$$\begin{aligned}
1 \cdot 120 + \ 0 \cdot 47 &= 120,\\
0 \cdot 120 + \ 1 \cdot 47 &= 47,\\
1 \cdot 120 - \ 2 \cdot 47 &= 26,\\
-1 \cdot 120 + \ 3 \cdot 47 &= 21,\\
2 \cdot 120 - \ 5 \cdot 47 &= 5,\\
-9 \cdot 120 + 23 \cdot 47 &= 1.
\end{aligned}$$

L'esponente cercato è quindi $E = 23$.

Esercizio 0.5. *Si consideri il sistema RSA di modulo* $n = 143 = 11 \cdot 13$ *ed esponente pubblico* $E = 37$.

(a) Cifrare il messaggio $m = 56$. *Calcolare cioè il resto, che si denoterà* $\widetilde{m}$, *della divisione per* 143 *del numero* 56^{37}.

(b) Decifrare il messaggio $\widetilde{m}$. *Calcolare cioè l'esponente segreto* D *tale che* $\widetilde{m}^D \equiv m \ mod\ 143$.

(a) Si ha che $56 \equiv 1 \bmod 11$, e quindi $56^{37} \equiv 1 \bmod 11$. Inoltre, $37 \equiv 1 \bmod 12$, da cui $56^{37} \equiv 4^{37} \equiv 4^1 \equiv 4 \bmod 13$. Ne segue che il resto della divisione per 143 di 56^{37} è il numero intero x, con $0 \leq x \leq 142$, che soddisfa il sistema di congruenze

$$\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv 4 \bmod 13. \end{cases}$$

Tale numero risulta $x = 56$, per cui in questo caso particolare $m = \widetilde{m} = 56$.

(b) In questo caso particolare, per il fatto che $m = \widetilde{m}$, è evidente che $D = 1$ soddisfa le condizioni richieste. In generale, l'esponente segreto D è l'inverso di 37 modulo $(11-1)(13-11) = 10 \cdot 12 = 120$ e si calcola risolvendo la congruenza

$$37x \equiv 1 \bmod 120.$$

Con l'algoritmo euclideo si trova

$$\mathrm{mcd}(37, 120) = 1, \qquad 37 \cdot 13 + (-4) \cdot 120 = 1,$$

per cui l'esponente segreto risulta $D = 13$. L'esponente cercato è quindi $E = 23$.

Esercizio 0.6. *Si consideri il sistema crittografico RSA di modulo* $143\ (= 11 \cdot 13)$ *ed esponente* $D = 113$. *(a) Cifrare il messaggio "54", cioè calcolare il resto della divisone per 143 del numero* 54^{113}.

(b) Determinare un esponente E *che consenta di decifrare il messaggio precedente. In altre parole, determinare un numero naturale* E *tale che* $(54^{113})^E \equiv 54$ *(mod 143).* (a) Osserviamo

che $x \equiv 54^{113} \bmod 143$ se e solo se

$$\begin{cases} x \equiv 54^{113} \bmod 11 \\ x \equiv 54^{113} \bmod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv (-1)^{113} \bmod 11 \\ x \equiv 2^{113} \bmod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv (-1)^3 \bmod 11 \\ x \equiv 2^5 \bmod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv -1 \bmod 11 \\ x \equiv 6 \bmod 13. \end{cases}$$

Per calcolare le potenze qui sopra, abbiamo usato il fatto che il gruppo moltiplicativo $\mathbb{Z}_{11}^*$ ha ordine 10, che il gruppo moltiplicativo $\mathbb{Z}_{13}^*$ ha ordine 12 e poi abbiamo applicato il teorema di Lagrange (Piccolo Teorema di Fermat).

Le soluzioni del sistema di congruenze $\begin{cases} x \equiv -1 \bmod 11 \\ x \equiv 6 \bmod 13 \end{cases}$ sono date da tutti gli interi della forma $x = 32 + k143,\ k \in \mathbb{Z}$. Il resto cercato è dunque 32 (compreso fra 0 e 143) e il messaggio cifrato risulta appunto $\widetilde{m} = 32$. (b) L'esponente cercato si trova risolvendo la congruenza

$$113 \cdot E \equiv 1 \bmod (11-1)(13-1) \quad \Leftrightarrow \quad 113 \cdot E \equiv 1 \bmod 120.$$

Poiché $mcd(113, 120) = 1$, la congruenza ha soluzione. Usando l'algoritmo euclideo, troviamo ad esempio $E = 17$.

Esercizio 0.7. *Si consideri il sistema RSA di modulo* $n = 143 = 11 \cdot 13$ *ed esponente pubblico* $E = 37$.

(a) Cifrare il messaggio $m = 56$*. Calcolare cioè il resto, che si denoterà* $\widetilde{m}$*, della divisione per* 143 *del numero* 56^{37}*.*

(b) Decifrare il messaggio $\widetilde{m}$*. Calcolare cioè l'esponente segreto* D *tale che* $\widetilde{m}^D \equiv m$ *mod* 143.
(a) Si ha che $56 \equiv 1 \bmod 11$, e quindi $56^{37} \equiv 1 \bmod 11$. Inoltre, $37 \equiv 1 \bmod 12$, da cui

$56^{37} \equiv 4^{37} \equiv 4^1 \equiv 4 \bmod 13$. Ne segue che il resto della divisione per 143 di 56^{37} è il numero intero x, con $0 \leq x \leq 142$, che soddisfa il sistema di congruenze

$$\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv 4 \bmod 13. \end{cases}$$

Tale numero risulta $x = 56$, per cui in questo caso particolare $m = \widetilde{m} = 56$.

(b) In questo caso particolare, per il fatto che $m = \widetilde{m}$, è evidente che $D = 1$ soddisfa le condizioni richieste. In generale, l'esponente segreto D è l'inverso di 37 modulo $(11-1)(13-11) = 10 \cdot 12 = 120$ e si calcola risolvendo la congruenza

$$37x \equiv 1 \bmod 120.$$

Con l'algoritmo euclideo si trova

$$\mathrm{mcd}(37, 120) = 1, \qquad 37 \cdot 13 + (-4) \cdot 120 = 1,$$

per cui l'esponente segreto risulta $D = 13$.

Esercizio 0.8. Nel sistema crittografico RSA di modulo $91 (= 7 \cdot 13)$ e esponente pubblico $D = 23$, si consideri il messaggio $m = 55$.
(a) Codificare il messaggio m. In altre parole, calcolare il resto di 55^{23} rispetto alla divisione per 91.
(b) Calcolare l'esponente di decodifica E. In altre parole: determinare $E > 0$ tale che $(a^{23})^E \equiv a \pmod{91}$ per ogni a tale che $mcd(a, 91) = 1$.

Soluzione. (a) Cerchiamo il numero intero x tale che $0 \leq x < 91$ e $x \equiv 55^{23} \pmod{91}$. Dunque $\begin{cases} x \equiv 55^{23} \pmod 7 \\ x \equiv 55^{23} \pmod{13} \end{cases}$.

Riduciamo 55^{23} modulo 7: $55 \equiv -1 \pmod 7$. Quindi $55^{23} \equiv -1 \pmod 7$.

Ora riduciamo 55^{23} modulo 13: $55 \equiv 3 \pmod{13}$. Dunque $55^{23} \equiv 3^{23} \pmod{13}$. Ora, usando le nota conseguenza del Teorema di Fermat, dobbiamo ridurre 23 modulo $12 (= 13 - 1)$. Si ha che

$$12 \equiv -1 \equiv 11 \pmod{12}$$

Dunque $3^{23} \equiv 3^{-1} \pmod{13}$, dove con $3^{-1} \pmod{13}$ si intende l'inverso di 3 modulo 13. Poichè l'inverso di 3 modulo 13 è 9 (infatti $3 \cdot 9 = 27 \equiv 1 \pmod{13}$), si ha, in definitiva, che

$$55^{23} \equiv 9 \pmod{13}.$$

Alternativamente, si può calcolare $3^2 = 9$, $3^3 = 27 \equiv 1 \pmod{13}$. Dunque $3^{11} = (3^3)^2 3^2 = 1 \cdot 9 = 9 \pmod{13}$.

Dunque dobbiamo risolvere il sistema $\begin{cases} x \equiv -1 \pmod 7 \\ x \equiv 9 \pmod{13} \end{cases}$. Si vede facilmente che la più piccola soluzione positiva, cioè il resto cercato, è $r = 48$.

Esercizio 0.9. Nel sistema crittografico RSA di modulo $91(= 7 \cdot 13)$ e esponente pubblico $D = 23$, si consideri il messaggio $m = 55$.
(a) Codificare il messaggio m. In altre parole, calcolare il resto r di 55^{23} rispetto alla divisione per 91.
(b) Stabilire (motivando) se si sarebbe potuto usare il messaggio $m' = 39$. Stabilire (motivando) se si sarebbe potuto usare l'esponente $D' = 27$.

Soluzione. (a) Cerchiamo il numero intero x tale che $0 \leq x < 91$ e $x \equiv 55^{23} \pmod{91}$. Dunque $\begin{cases} x \equiv 55^{23} \pmod 7 \\ x \equiv 55^{23} \pmod{13} \end{cases}$.

Riduciamo 55^{23} modulo 7: $55 \equiv -1 \pmod 7$. Quindi $55^{23} \equiv -1 \pmod 7$.

Ora riduciamo 55^{23} modulo 13: $55 \equiv 3 \pmod{13}$. Dunque $55^{23} \equiv 3^{23} \pmod{13}$. Ora, usando le nota conseguenza del Teorema di Fermat, dobbiamo ridurre 23 modulo $12(= 13 - 1)$. Si ha che

$$12 \equiv -1 \equiv 11 \pmod{12}$$

Dunque $3^{23} \equiv 3^{-1} \pmod{13}$, dove con $3^{-1} \pmod{13}$ si intende l'inverso di 3 modulo 13. Poichè l'inverso di 3 modulo 13 è 9 (infatti $3 \cdot 9 = 27 \equiv 1 \pmod{13}$), si ha, in definitiva, che

$$55^{23} \equiv 9 \pmod{13}.$$

Alternativamente, si può calcolare $3^2 = 9$, $3^3 = 27 \equiv 1 \pmod{13}$. Dunque $3^{11} = (3^3)^2 3^2 = 1 \cdot 9 = 9 \pmod{13}$.

Dunque dobbiamo risolvere il sistema $\begin{cases} x \equiv -1 \pmod 7 \\ x \equiv 9 \pmod{13} \end{cases}$. Si vede facilmente che la più piccola soluzione positiva, cioè il resto cercato, è $r = 48$.

(b) NON si sarebbe potuto usare il messaggio $m' = 39$, perchè $mcd(39, 91) > 1$.

NON si sarebbe potuto usare l'esponente $D' = 27$ perché $mcd(27, 72) > 1$ (dove $72 = (7 - 1)(13 - 1)$).