Prof. Maurizio Dècina

CRITTOGRAFIA E SICUREZZA

Prima Prova del 7-5-2007 (un ora e trenta minuti di tempo)

Quesito 1

Dato il campo finito **GF**(2^4) in $\mathbf{Z}_2$[x]mod p(x), ove p(x)= $x^4 + x^3 + 1$,:

1. verificare che p(x) è un *polinomio primitivo*,
2. determinare le sue *radici primitive*,
3. determinare gli *inversi* delle radici primitive,
4. indicare quanti e quali sono i *residui quadratici* del campo,
5. verificare che il *polinomio irriducibile*: r(x)= $x^4 + x^3 + x^2 + x + 1$ *non* è primitivo.

Quesito 2

Siano date le seguenti due *congruenze*, ove tutti gli interi indicati sono primi,

a - $x^2 \equiv 43 \pmod{179}$,
b - $x^2 \equiv 1093 \pmod{65537}$.

Utilizzando per ambedue le congruenze i *simboli di Legendre/Jacobi*:

1. verificare se esiste soluzione, e,
2. se possibile, determinare i valori di x.

Quesito 3

Dato il campo finito **GF**(2^3) in $\mathbf{Z}_2$[x](mod $x^3 + x + 1$) si cifri il messaggio in chiaro binario P = 101001001110 con un *cifrario di Hill* caratterizzato dalla matrice 2x2 : $\mathbf{K} = \begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix}$.

1. Quali condizioni deve rispettare la chiave **K**?
2. Qual'è il messaggio cifrato binario C?
3. Decifrare il messaggio cifrato ottenuto al passo precedente.
4. Usando la coppia messaggio in chiaro, messaggio cifrato ottenuta ai punti precedenti effettuare un attacco *known plaintext* e ricavare la chiave **K**.

Quesito 4

Si consideri un testo in chiaro composto dalle 26 lettere maiuscole dell'alfabeto inglese, numerate da 0 a 25. Alice e Bob usano il *crittosistema di Rabin* e adottano come chiave pubblica n=77 e come chiave privata segreta la fattorizzazione $n=p\cdot q = 7\cdot 11$. Alice cifra a caratteri isolati (ECB) il messaggio in chiaro P = P_1,P_2 = KY = 10,24 e lo invia a Bob.

1. Con quali interi C_1,C_2 mod n, Alice cifra il messaggio in chiaro?
2. Come decifra Bob correttamente il messaggio cifrato C_1,C_2 inviato da Alice?
3. Oscar effettua un attacco *chosen chiphertext* basato su C_1 e ha a disposizione il decifratore di Alice per alcune prove; in corrispondenza di C_1 il decifratore restituisce due *plaintext:* P_1mod77 e $P_x$mod77, tali che risulta $\pm P_1 \neq \pm P_x$ (mod77); come fa Oscar a determinare la chiave privata e quindi a decifrare C_2?

PUNTEGGI: Quesito 1=5 punti; Quesito 2=7 punti; Quesito 3=11 punti; Quesito 4=7 punti.

Usare un foglio diverso per quesito con
 # Quesito, Nome, Cognome, # Matricola, Data, Firma

QUESITO 1

$GF(2^4)$ in $\mathbb{Z}_2[x]\,(\bmod\ x^4+x^3+1)$

$p(x)=0$ per $x_i=\alpha^{2^{i-1}}$; $1\le i\le 4$

residui 0
- α
- α^2
- α^3
- $\alpha^4=\alpha^3+1$
- $\alpha^5=\alpha^3+\alpha+1$
- $\alpha^6=\alpha^3+\alpha^2+\alpha+1$
- $\alpha^7=\alpha^2+\alpha+1$
- $\alpha^8=\alpha^3+\alpha^2+\alpha$
- $\alpha^9=\alpha^2+1$
- $\alpha^{10}=\alpha^3+\alpha$
- $\alpha^{11}=\alpha^3+\alpha^2+1$
- $\alpha^{12}=\alpha+1$
- $\alpha^{13}=\alpha^2+\alpha$
- $\alpha^{14}=\alpha^3+\alpha^2$
- $\alpha^{15}=1$

2. - la prima radice primitiva è $x=\alpha$: infatti
   $\alpha^4+\alpha^3+1=\alpha^3+1+\alpha^3+1=0$
   - la seconda è $x=\alpha^2$: infatti
   $\alpha^8+\alpha^6+1=\alpha^3+\alpha^2+\alpha+\alpha^3+\alpha^2+\alpha+1+1=0$
   - la terza è $x=\alpha^4$
   $\alpha^{16}+\alpha^{12}+1=\alpha+\alpha+1+1=0$
   - la quarta è $x=\alpha^8$
   $\alpha^{32}+\alpha^{24}+1=\alpha^2+\alpha^2+1+1=0$

$\boxed{\begin{array}{l} \alpha^{K}\equiv\alpha^{K \bmod 15} \\ \text{per } K>15\end{array}}$

1. per verificare che $p(x)$ è primitivo bisogna verificare che l'ordine di $x=\alpha$ è 2^4-1 e cioè che $2^4-1=15$ è il minimo esponente di α tale che $\alpha^K=1$ OK per $K=15$. $(\bmod\ p(x))$

$\boxed{\begin{array}{l} 2^4-1=15 \\ \beta\equiv(\alpha)^i \quad 1\le i\le 15\end{array}}$

3 gli elementi inversi sono $(\alpha^i)^{2^4-2}\,(\bmod\ x^4+x^3+1)\equiv(\alpha^i)^{14}\xrightarrow{\text{vedi retro}}$

4. i residui quadratici sono $2^4/2=8$
$(\alpha^2,\alpha^4,\alpha^6,\alpha^8,\alpha^{10},\alpha^{12},\alpha^{14},1)$

5. Per verificare che $r(x)$ non è primitivo basta verificare che
$$\cancel{x}^{K}\equiv 1\ (\bmod\ r(x))$$
per $K<2^n-1$. Si parte da
$$x^4\equiv x^3+x^2+x+1\quad(\bmod\ r(x))$$
per cui, moltiplicando per x si trova subito
$$x^5\equiv x^4+x^3+x^2+x\equiv x^3+x^2+x+1+x^2\cancel{x^2}+x\equiv$$
$$\equiv 1.$$
e cioè $K=5$ è l'ordine di x in $\mathbb{Z}[x]\,\bmod r(x))$ <15 quindi $r(x)$ ~~non~~ è primitivo.

Aritmetica

$p(x)=x^4+x^3+1$

$\boxed{\alpha^4=\alpha^3+1}$

Residui

$\alpha^i \quad 1\le i\le 2^4-1$

Inversi

$(\alpha^i)^{2^4-2}\equiv(\alpha^i)^{14}$ $(\bmod x^4+x^3+1)$ $1\le i\le 2^4-1$

$\frac{2^4}{2}=8$ Residui quadratici (i pari + $i=1$)

	α	● radice di $p(x)$	$\alpha^{14}=\alpha^{14}$	$14\equiv14$
→	● α^2	● radice di $p(x)$	$\alpha^{28}=\alpha^{13}$	$28\equiv13$
	α^3		$\alpha^{42}=\alpha^{12}$	$42\equiv12$
→	● α^4	● radice di $p(x)$	$\alpha^{56}=\alpha^{11}$	$56\equiv11$
	α^5		$\alpha^{70}=\alpha^{10}$	$70\equiv10$
→	● α^6		$\alpha^{84}=\alpha^9$	$84\equiv9$
	α^7		$\alpha^{98}=\alpha^8$	$98\equiv8$
→	● α^8	● radice di $p(x)$	$\alpha^{112}=\alpha^7$	$112\equiv7$
	α^9		$\alpha^{126}=\alpha^6$	$126\equiv6$
→	● α^{10}		$\alpha^{140}=\alpha^5$	$140\equiv5$
	α^{11}		$\alpha^{154}=\alpha^4$	$154\equiv4$
→	● α^{12}		$\alpha^{168}=\alpha^3$	$168\equiv3$
	α^{13}		$\alpha^{182}=\alpha^2$	$182\equiv2$
→	● α^{14}		$\alpha^{196}=\alpha$	$196\equiv1$
→	$\alpha^{15}\equiv1$		$\alpha^{210}=1$	$210\equiv0$

mod 15

Il polinomio è primitivo in quanto 15 è l'ordine di α! $\quad 15=2^4-1$

Le radici di $p(x)=0$ sono $n=4$

$$x_i=\alpha^{2^{i-1}} \text{ per } 1\le i\le 4$$

$$(\alpha;\alpha^2;\alpha^4;\alpha^8)\ (\bmod p(x))$$

Cifrario di Hill $GF(2^3)$ in $\mathbb{Z}_2[x]$ (mod x^3+x+1) **QUESITO 3** ①

$P = 101\ 001\ 001\ 110$

$K = \begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix}$

$P = (x^2+1),(1),(1),(x^2+x)$

000	0
001	1
010	x
011	$x+1$
100	x^2
101	x^2+1
110	x^2+x
110	x^2+x+1

1. $\det K = x^2+x+1 \neq 0$ e $\mathrm{mcd}(x^2+x+1, x^3+x+1) = 1$

$\det K^{-1} = \dfrac{1}{x^2+x+1} = x^2$ (mod x^3+x+1) infatti

$$\begin{array}{l|l} & 0 \\ & 1 \\ \hline x^3+x+1 = (x^2+x+1)(x+1) + x & x+1 \\ x^2+x+1 = (x+1)x \quad + 1 & (x^2+1)^2+1 = x^2 \end{array}$$

$$K^{-1} = x^2\begin{pmatrix} 1 & -1 \\ -(x+1) & x^2 \end{pmatrix} = \begin{pmatrix} x^2 & \cancel{x}^2 \\ x^3+x^2 & x^4 \end{pmatrix} = \begin{pmatrix} x^2 & x^2 \\ x^2+x+1 & x^2+x \end{pmatrix}$$

verifica

$$K \cdot K^{-1} = \begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix}\begin{pmatrix} x^2 & x^2 \\ x^2+x+1 & x^2+x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ ok}$$

2. ciphering $C = KP$

$$C = \begin{pmatrix} x^2+1 & 1 \\ 1 & x^2+x \end{pmatrix}\begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x^2 \\ x^2+1 & x^2+x+1 \end{pmatrix}$$

$C = (1),(x^2),(x^2+1),(x^2+x+1) = 001\ 100\ 101\ 111$

$\det P = x \neq 0$ e $\mathrm{mcd}(x, x^3+x+1) = 1$

$\det C = x^2+1 \neq 0$ e $\mathrm{mcd}(x^2+1, x^3+x+1) = 1$

3. Deciphering $P = CK^{-1}$

$$P = \begin{pmatrix} 1 & x^2 \\ x^2+1 & x^2+x+1 \end{pmatrix}\begin{pmatrix} x^2 & x^2 \\ x^2+x+1 & x^2+x \end{pmatrix} = \begin{pmatrix} x^2+1 & 1 \\ 1 & x^2+x \end{pmatrix} \text{ ok}$$

4. Attacco known plaintext ②

$$\begin{pmatrix} x^2+1 & 1 \\ 1 & x^2+x \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & x^2 \\ x^2+1 & x^2+x+1 \end{pmatrix}$$

$(\bmod\ x^3+x+1)$

deve essere $ad-bc \neq 0$ e $\text{mcd}((ad-bc), x^3+x+1)=1$

inverto P e trovo $K = P^{-1}C$

$\det P = x$ $\quad \det P^{-1} = x^2+1$ $\quad (x^2+1)x = x^3+x = 1$

$$P^{-1} = (x^2+1)\begin{pmatrix} x^2+x & -1 \\ -1 & x^2+1 \end{pmatrix} = \begin{pmatrix} x+1 & x^2+1 \\ x^2+1 & x^2+x+1 \end{pmatrix}$$

$$K = \begin{pmatrix} x+1 & x^2+1 \\ x^2+1 & x^2+x+1 \end{pmatrix}\begin{pmatrix} 1 & x^2 \\ x^2+1 & x^2+x+1 \end{pmatrix} = \begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix}$$ chiave trovata.

verifica $$P \cdot P^{-1} = \begin{pmatrix} x^2+1 & 1 \\ 1 & x^2+x \end{pmatrix}\begin{pmatrix} x+1 & x^2+1 \\ x^2+1 & x^2+x+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ok.

QUESITO 4

$7 \equiv 11 \equiv 3 \pmod 4$

1. $P_1 = 10 = K$ $C_1 = 10^2 \bmod 77 = 23 = C_1$

$n = 77;\ p = 7;\ q = 11$

la radice quadrata di 23

$x^2 \equiv 23 \pmod{77}$

$a_1^2 = 23 \bmod 7 \equiv 2 \bmod 7$

$a_2^2 = 23 \bmod 11 = 1 \bmod 11$

$a_1 = 2^{\frac{7+1}{4}} = 4 \bmod 7$ Radici $\pm a_1 \equiv \pm 4 \bmod 7$

$a_2 = 1 \bmod 11$ $\pm a_2 \equiv \pm 1 \bmod 11$

$z_1 = 7\ ;\ z_2 = 11$ $y_1 = 11^{-1} \bmod 7 \equiv 11^5 \equiv 2 \pmod 7$

$x = \sum_i (\pm a_i) y_i z_i \pmod n$ $y_2 = 7^{-1} \bmod 11 \equiv 7^9 \equiv 8 \pmod{11}$

allora

$x_1\ (+a_1, +a_2)$ $x_1 = 4 \times 2 \times 11 + 1 \times 8 \times 7 = 144 = 67 \overset{\equiv 10}{\wedge} \pmod{77}$

$x_2\ (-a_1, +a_2)$ $x_2 = -88 + 56 = \underline{-32} = 45$

$x_3 = 88 - 56 = \underline{32}$ $x_3 = -x_2$

$x_4 = -88 - 56 = -144 = -67 = \underline{10}$ $x_4 = -x_1$

Le radici di 23 mod 77 sono $(10, 32, 45, 67)$ e Bob sceglie 10 – in modo che $0 \leq 10 \leq 25$ e le altre soluzioni sono > 25. $(10, -10, 32, -32)$

$(\pm 10$ e $\pm 32 \bmod 77)$ $P_1 = 10 = K$. ok

---

2. $P_2 = Y = 24$ $C_2 = 24^2 = 576 \bmod 77 = 37 = C_2$ $x^2 = 37 \pmod{77}$

$a_1^2 = 37 \bmod 7 = 2 \bmod 7$

$a_2^2 = 37 \bmod 11 = 4 \bmod 11$ $a_1 = 4 \bmod 7$ $\pm a_1 \equiv \pm 4 \bmod 7$

$a_2 = 4^2 = 16 \bmod 7 = 2$ $\pm a_2 \equiv \pm 2 \bmod 11$

$z_1 = 7$ $z_2 = 11$ $y_1 = 2 \bmod 7\ ;\ y_2 = 8 \bmod 11$

$X_1 = (+a_1, +a_2)$ $x_1 = 4 \cdot 2 \cdot 11 + 2 \cdot 8 \cdot 7 = 88 + 112 = 200 = 46$

$x_2 = -88 + 112 = 24$ $\pmod{77}$

$x_3 = 88 - 112 = -24$

$x_4 = -88 - 112 = -200 = -46$

le radici sono $(\pm 24\ \ \pm 46)$

Bob sceglie 24 $P_2 = 24 = Y$. ok

3. Oscar ha $C_1 = 23 \bmod 77$ e non conosce la fattorizzazione $77 = 7 \cdot 11$, e cioè $p = 7$ e $q = 11$. Infatti C_1 nel decifrare di Alice e riceve. Ad esempio due plaintext $10 \bmod 77$ (P_1) e $45 = P_X \pmod{77}$ che corrispondono a due radici diverse di 23 mod 77 $\pm 45 \not\equiv \pm 10 \pmod{77}$. Allora calcola

$$mcd(45-10, 77) = mcd(35, 77) = 7 = p$$ BINGO!

e quindi $q = \frac{n}{p} = \frac{77}{7} = 11$.

Scoperta la trapdoor Oscar decifra agevolmente C_2 in $P_2 = 24 \bmod 77$, come ha fatto Bob.

Prof. Maurizio Dècina

INTERNET: INFRASTRUTTURE E SICUREZZA (Milano)

Prova Intermedia del 21-11-2005 (due ore di tempo)

SICUREZZA DELLE RETI INTERNET (Como)

Prova del 21-11-2005 (due ore di tempo)

Quesito 1

Sia dato un alfabeto composto da 256 simboli (byte di 8 bit). Bob decide di utilizzare soltanto i 128 caratteri numerati da 0 a 127, e di impiegare un algoritmo di *'cifratura a catena'* definito dalle equazioni:

$$[1] \qquad Z_i = E_K(P_{i-1} \oplus C_{i-1})$$
$$C_i = E_K(Z_i \oplus P_i); \qquad i=1,2;\ C_0=00000001\ ;\ P_0=00000001.$$

a) Descrivere l'operazione di cifratura e decifratura che trasforma due simboli in chiaro P_1, P_2 in due simboli cifrati C_1, C_2 e viceversa, sia in forma di schemi a blocchi che con equazioni del tipo [1].

Bob decide inoltre di adottare per la funzione $E_K(x)$ il *sistema di cifratura RSA*. Egli pubblica i parametri:

$$m = 221;\ b = 25$$

e le equazioni [1], inclusi i valori di inizializzazione P_0 e C_0. Bob mantiene il segreto sulla *trapdoor:* $m=p.q=13.17.$

b) Verificare la validità dei parametri *m, b* pubblicati da Bob, secondo RSA, e calcolare il parametro $a=b^{-1}$.

c) Cifrare i simboli $P_1=3$, $P_2=3$ (Alice cifra con la chiave pubblica di Bob).

d) Decifrare i simboli C_1, C_2 risultato della domanda precedente (Bob decifra con la chiave privata).

e) Si supponga che Oscar intercetti C_1, C_2 e conosca le informazioni rese pubbliche da Bob. Determinare la complessità dell'attacco, in termini di numero di tentativi, per i valori numerici di questo esercizio.

N:B: Riportare il calcolo degli esponenziali modulari complessi secondo il metodo adottato (S & M, Euclide esteso, riduzioni esponenziali)

Quesito 2

Bob adotta lo schema di *'firma di ElGamal'* e sceglie $p=97$. Pubblica quindi i valori:

$$p = 97;\ \alpha = 5;\ \beta = ?$$

e tiene segreti i valori:

$$a = 13;\ k = 95.$$

a) Enunciare le ipotesi dello schema di *firma di ElGamal* per i parametri (p, a, k): quanti sono i possibili valori di P, di k e di a?

b) Dire quanti sono gli elementi primitivi $\in Z^*_p$ e verificare che $\alpha=5$ è un elemento primitivo di Z^*_p.

c) Determinare il valore di β.

d) Qual e' la firma del messaggio in chiaro $P=31$?

e) Verificare la firma determinata al punto precedente.

f) Quante firme diverse sono possibili in base ai dati numerici di questo esercizio?

N:B: Riportare il calcolo degli esponenziali modulari complessi secondo il metodo adottato (S & M, Euclide esteso, riduzioni esponenziali)

Quesito 3

Eseguire la *sostituzione del byte di stato AES* espresso in esadecimale $\{95\}_{hex}$, secondo *l'algoritmo Rijndael "SUBBYTES"*.

a) Inversione: il polinomio irriducibile nel Campo di Galois GF(2^8) è: $m(x) = x^8+x^4+x^3+x+1$.

b) Verifica della inversione.

c) Sostituzione:

$$SUBBYTES_{AES}(a_i) \Rightarrow b_i = (a_i + a_{i+4} + a_{i+5} + a_{i+6} + a_{i+7} + c_i\ )mod2, \quad per\ 0 \leq i \leq 7,$$

avendo assunto di calcolare gli indici $(i+X)$ modulo 8, per $X=4;5;6;7$ e il byte di inizializzazione $C=(c_i)=\{63\}_{hex}$.

Quesito 4

Si illustri *l'attacco del compleanno* ai codici "hash".

a) Descrivere le modalità dell'attacco e lo scopo truffaldino dell'attaccante.

b) Ricavare la formula approssimata del paradosso del compleanno.

c) Determinare la complessità degli attacchi, in termini di numero di tentativi, ai codici hash corrispondenti: ai "cookies", allo standard MD5 e a quello SHA-1.

Quesito 5

Illustrare la sequenza dei messaggi scambiati tra Alice e Bob nel *protocollo autenticato per l'accordo sulle chiavi*.

a) Descrivere il protocollo di Diffie e Hellman, D-H.

b) Descrivere l'attacco "man in the middle", MITM, al protocollo D-H.

c) Illustrare il protocollo "simple station to station", SSS.

d) Aggiungere al protocollo SSS la prestazione di "conferma mutua del possesso della chiave".

e) Aggiungere al protocollo SSS la prestazione di resilienza agli attacchi "denial of service", DOS.

f) Aggiungere al protocollo SSS il "fix" contro gli "attacchi della replica", "reply attack".

PUNTEGGI: Quesito 1=7 punti; Quesito 2=8 punti; Quesito 3=4 punti; Quesito 4=4 punti; Quesito 5=7 punti.

QUESITO 3

altro esempio

2

$$\mathbb{F}_{2^8} \equiv GF(2^8) \equiv \mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$$

$$1001\ 0101 \rightarrow \boxed{95}_{hex}$$

$$a(x) = (x^7+x^4+x^2+1) \qquad a^{-1}(x)$$

$r_0 = m(x)$

$r_1 = a(x)$

$r_2 = x^5+x^4+1$

$q_1 = x$

$q_2 = x^2+x+1$

$r_3 = x$

$q_3 = x^4+x^3$

$r_4 = 1 \quad 4 \equiv MAX$

$t_0 = 0;\ t_1 = 1$

$t_2 = t_0 - q_1 t_1 =$

$= 0 - x = x$

$t_3 = t_1 - q_2 t_2 =$

$= 1 - (x^2+x+1)(x) =$

$= x^3+x^2+x+1$

$t_4 = t_2 - q_3 t_3 =$

$$\begin{array}{r|l} & x \\ x^7+x^4+x^2+1 & x^8+x^4+x^3+x+1 \\ & x^8+x^5+x^3+x \\ \hline & x^5+x^4 \quad +1 \end{array}$$

$$\begin{array}{r|l} & x^2+x+1 \\ x^5+x^4 \quad +1 & x^7+x^4+x^2+1 \\ & x^7+x^6+ \quad x^2 \\ \hline & x^6+x^4+1 \\ & x^6+x^5+x \\ \hline & x^5+x^4+x+1 \\ & x^5+x^4+1 \\ \hline & x \end{array}$$

$$\begin{array}{r|l} & x^4+x^3 \\ x & x^5+x^4+1 \\ & x^5 \\ \hline & x^4+1 \\ & x^4 \\ \hline & 1 \end{array}$$

$$x - (x^4+x^3)(x^3+x^2+x) = x + x^7 + \cancel{x^6} + \cancel{x^5} + \cancel{x^6} + \cancel{x^5} + \cancel{x^4} + \cancel{x^4} + x^3$$

$$a^{-1}(x) = x^7+x^3+x \qquad = x^7+x^3+x = a^{-1}(x) \quad 10001010 \quad \boxed{BA}_{hex}$$

verifica

$$(x^7+x^3+x)(x^7+x^4+x^2+1) \equiv 1 \mod (x^8+x^4+x^3+x+1)$$

$$(x^7+x^3+x)(x^7+x^4+x^2+1) =$$

$$x^{14}+x^{11}+x^9+\cancel{x^7}+x^{10}+\cancel{x^7}+\cancel{x^5}+\cancel{x^3}+$$

$$x^8+\cancel{x^5}+\cancel{x^3}+x =$$

$$x^6+x^3+x^{11}$$

$$x^8+x^4+x^3+x+1 \,\big/\, x^{14}+x^{11}+x^{10}+x^9+x^{\overset{8}{0}}+x$$

$$\underline{x^{14}+x^{10}+x^9+x^7+x^6}$$

$$x^{11}+x^8+x^7+x^6+x$$

$$\underline{x^{11}+x^7+x^6+x^4+x^3}$$

$$x^8+x^4+x^3+x$$

$$\underline{x^8+x^4+x^3+x+1}$$

1 OK

$c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0$
$0\ 1\ 1\ 0\ 0\ 0\ 1\ 1$

$c \equiv \{63\} = 0110\ 0011$

$\{8A\}\quad 10001010$

$a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0$
$1\ 0\ 0\ 0\ 1\ 0\ 1\ 0$

$b_0 = a_0 + a_4 + a_5 + a_6 + a_7 + c_0 = 0$
$0 + 0 + 0 + 0 + 1 + 1$

$b_1 = a_1 + a_5 + a_6 + a_7 + a_0 + c_1 = 1$
$1 + 0 + 0 + 1 + 0 + 1$

$b_2 = a_2 + a_6 + a_7 + a_0 + a_1 + c_2 = 0$
$0 + 0 + 1 + 0 + 1 + 0$

$b_3 = a_3 + a_7 + a_0 + a_1 + a_2 + c_3 = 1$
$1 + 1 + 0 + 1 + 0 + 0$

$b_4 = a_4 + a_0 + a_1 + a_2 + a_3 + c_4 = 0$
$0 + 0 + 1 + 0 + 1 + 0$

$b_5 = a_5 + a_1 + a_2 + a_3 + a_4 + c_5 = 1$
$0 + 1 + 0 + 1 + 0 + 1$

$b_6 = a_6 + a_2 + a_3 + a_4 + a_5 + c_6 = 0$
$0 + 0 + 1 + 0 + 0 + 1$

$b_7 = a_7 + a_3 + a_4 + a_5 + a_6 + c_7 = 0$
$1 + 1 + 0 + 0 + 0 + 0$

$\{95\} \rightarrow \boxed{S\text{-}AES} \rightarrow \{2A\}$

$\text{SUBBYTE}_{AES}\{95\} \equiv 0010\ 1010 = \{2A\}$
$\{2\ \ A\}$

$\text{SUBBYTES}_{AES}\{95\} = \{2A\}$.

Prof. Maurizio Dècina

CRITTOGRAFIA E SICUREZZA

Primo Applello del 9-7-2007 (due ore e quindici minuti di tempo)

Quesito 1

Verificare se il numero intero n = 561 è primo utilizzando il **test di Fermat** e il **test di Miller Rabin** con basi a = 2 e a = 3.

1. Test di Fermat.
2. Test di Miller-Rabin e fattorizzazione di n.

Quesito 2

Si consideri un testo in chiaro composto dalle 26 lettere maiuscole dell'alfabeto inglese, numerate da 0 a 25. Alice e Bob usano il **crittosistema di Rabin** e adottano come chiave pubblica n=57 e come chiave privata segreta la fattorizzazione n=p·q =3·19. Alice cifra a caratteri isolati (ECB) il messaggio in chiaro P_1= G= 7; P_2= K=10, e lo invia a Bob.

1. Con quali interi, C_1, C_2 mod n, Alice cifra il messaggio in chiaro, P_1, P_2?
2. Come decifra Bob il messaggio cifrato C_1 inviato da Alice?
3. Come decifra Bob il messaggio cifrato C_2 inviato da Alice?
4. Oscar effettua un attacco *chosen chiphertext* basato su C_1 e ha a disposizione il decifratore di Alice per alcune prove; in corrispondenza di C_1 il decifratore restituisce due *plaintext:* P_1mod57 e $P_x$mod57, tali che risulta $\pm P_1 \neq \pm P_x$ (mod57); come fa Oscar a determinare la chiave privata e quindi a decifrare C_2?

Quesito 3

Sia dato il **campo finito** GF(2^3) in Z_2[x](mod x^3+ x^2 + 1). si cifri il messaggio in chiaro binario P = P_1, P_2 = (101, 010) con un **cifrario di Hill affine**: **C = P H + B**, ove B = B_1, B_2 = (100, 111) e la matrice 2x2: **H** = $\begin{pmatrix} 100 & 101 \\ 010 & 010 \end{pmatrix}$, avendo numerato in binario gli elementi polinomiali del campo.

1. Elencare gli elementi del campo, indicare le radici del polinomio primitivo p(x) = x^3+ x^2 + 1.
2. Quali condizioni deve rispettare la matrice **H**?
3. Determinare la matice $\mathbf{H^{-1}}$, e verificare.
4. Qual'è il messaggio cifrato binario C= C_1, C_2?
5. Decifrare il messaggio cifrato ottenuto al passo precedente.

Quesito 4

Utilizzando lo stesso **campo finito** del Quesito 3, realizzare un **crittosistema di ElGamal**, assumendo che: P,C $\in$ GF(2^3) (mod x^3+ x^2 + 1), mentre il segreto, a, di Bob e il nonce, k, di Alice sono numeri interi: $1 \leq a, k \leq (2^3-2)$.

Come radice primitiva del campo ciclico si utilizza x = α = 010. La chiave pubblica di Bob è $\beta = \alpha^a$. Bob pubblica: [GF(2^3) (mod x^3+ x^2 + 1), α, β] e tiene segreta la sua chiave a=3. Alice sceglie il nonce k = 4 e cifra il testo in chiaro P = 111.

1. Qual'è il testo cifrato C = (r, t), ove r, t $\in$ GF(2^3) (mod x^3+ x^2 + 1)?
2. Come decifra Bob il messaggio ricevuto C = (r, t)?

Quesito 5

Bob usa un **crittosistema di ElGamal** con il gruppo ciclico generato dalla **curva ellittica mod p**:

$$E : y^2 = x^3 + 3 \pmod 7$$

1. Determinare l'ordine N del gruppo ciclico. Quanti sono gli elementi primitivi?
2. Usare l'algoritmo *double & add* per verificare la moltiplicazione $N \cdot A = \infty$ del punto A =(3,4).
3. Determinare tutti gli elementi del gruppo.

Bob pubblica quindi E, *p*=7; *q* numero primo componente N, A=(3,4) e B=*a*A, e mantiene segreta la sua chiave *a*=3. Alice vuole inviare a Bob il testo in chiaro *P*=5A e sceglie il *nonce k*=4.

4. Qual'è il testo cifrato C = (Y_1,Y_2) inviato da Alice?.
5. Come decifra Bob il messaggio ricevuto C = (Y_1,Y_2)?

PUNTEGGI:

Quesito 1=4 punti; Quesito 2=6 punti; Quesito 3=7 punti; Quesito 4=4 punti; Quesito 5=9 punti.

Usare un foglio diverso per quesito con

 # Quesito, Nome, Cognome, # Matricola, Data, Firma

QUESITO 2
Crittosistema di Rabin

$n = p\cdot q$ $\quad p=3 \quad q=19 \quad n=57$

$p, q \equiv 3 \bmod 4$

Alice cifra il testo in chiaro

① $P \in \mathbb{Z}_{26} \to P_1 = 7$ $\qquad C_1 = P^2 = 49 \bmod 57$

Bob decifra conoscendo p e q

$a^2 = 49 = 11 \bmod 19$

$b^2 = 49 = 1 \bmod 3$

$a = 11^{\frac{19+1}{4}} \equiv 11^5 \equiv 7 \bmod 19$

$b = 1^{\frac{3+1}{4}} \equiv 1 \bmod 3$

$$\begin{cases} \pm a \equiv \pm 7 \bmod 19 \\ \pm b \equiv \pm 1 \bmod 3 \end{cases}$$

$p^{-1} = 3^{-1} \bmod 19 \equiv 3^{17} \equiv 13 \equiv -6$

$q^{-1} \equiv 19^{-1} \bmod 3 \equiv 19 \equiv 1 \bmod 3$

$a = 7 \bmod 19; \quad b = 1 \bmod 3$

$\begin{cases} a=7 \\ b=1 \end{cases}$ $\quad k = (a-b)\,3^{-1} \bmod 19 = 6\cdot 13 = 78 \equiv 2 \bmod 19$

x_1 $\quad x_1 = b + pk = 1 + 3\cdot 2 = 7 \bmod 57 \qquad x_1 = 7$

$x_2 = \begin{cases} a=7 \\ b=-1 \end{cases} \quad x_2 = 26 \qquad x_3 = \begin{cases} a=-7 \\ b=1 \end{cases} \quad x_3 = 31$

$x_4 \begin{cases} a=-7 \\ b=-1 \end{cases} \quad x_4 = 50 \qquad x \equiv [7, 26, 31(\equiv -26), 50(\equiv -7)]$

4 radici

Solo la $x = 7 \in \mathbb{Z}_{26}$ ok!

②

② $P_2 = 10$

$C_2 = 100 \bmod 57 = 43 \bmod 57$

$a^2 = 43 \bmod 19 = 5$

$b^2 = 43 \bmod 3 = 1$

$p = 3$

$q = 19$

$$\begin{cases} a = 5^{\frac{19+1}{4}} = 5^5 \equiv 9 \bmod 19 \\ b = 1 \bmod 3 \end{cases}$$

$\pm a = \pm 9$

$\pm b = \pm 1$

$3^{-1} = p^{-1} = -6 = 13_{\bmod 19}$ $\quad q^{-1} = 1 = 19^{-1}_{\bmod 3}$

$$\begin{cases} a = 9 \\ b = 1 \end{cases} \quad \begin{aligned} & k = (a-b)3^{-1} \bmod 19 = 8 \cdot 13 = 9 \bmod 19 \\ & X_1 = b + pk = 1 + 3 \cdot 9 = 28 \bmod 57 \end{aligned}$$

$X_1 = 28$

$$k = (\overset{9+1}{a-b})3^{-1} \bmod 19 = \underline{10} \cdot 13 = 16 \bmod 19$$

$$\begin{cases} a = 9 \\ b = -1 \end{cases} \quad X_2 = -1 + 3 \cdot 16 = 47 \bmod 57$$

$X_2 = 47$

$$k = (\overset{-9-1}{a-b})3^{-1} = 9 \cdot 13 = 3 \bmod 19$$

$$\begin{cases} a = -9 \\ b = 1 \end{cases} \quad X_3 = 1 + 3 \cdot 3 = 10 \bmod 57$$

$X = 10 = -47$

$$k = (\overset{-9+1}{a-b}) \cdot 3^{-1} = 11 \cdot 13 = 10 \bmod 19$$

$$\begin{cases} a = -9 \\ b = -1 \end{cases} \quad X_4 = -1 + 3 \cdot 10 = 29 \bmod 57$$

$X = 29 = -28$

$X \equiv (28, 47, 10, 29)$

$\underline{\underline{X}} = 10 \in \mathbb{Z}$

26

③ $\text{mcd}(26-7, 57) = 19$

QUESITO 3

Cifrario Hill Affine

Ⓣ

$$C = P\,H + B$$

$$(C_1\, C_2) = (P_1\, P_2)\underset{[4\times4]}{H} + (B_1, B_2)$$

$$P = (C - B)\,H^{-1}$$

in $GF(2^3)\ (\text{mod } x^3+x^2+1)$

0 000

• $\alpha^1 \equiv \alpha$ 010

• $\alpha^2 \equiv \alpha^2$ 100

$\alpha^3 \equiv \alpha^2+1$ 101

• $\alpha^4 \equiv \alpha^3+\alpha \equiv \alpha^2+\alpha+1$ 111

$\alpha^5 \equiv \alpha^3+\alpha^2+\alpha \equiv \alpha^2+1+\alpha^2+\alpha = \alpha+1$ 011

$\alpha^6 \equiv \alpha^2+\alpha$ 110

$\alpha^7 \equiv 1$ 001

$P = (101, 010)$

$P = (\alpha^3, \alpha) = (P_1, P_2)$

$B = (\alpha^2, \alpha^4) = (B_1, B_2)$

Le radici di x^3+x^2+1 sono: $\underline{\alpha}, \underline{\alpha^2}, \underline{\alpha^4}$ (sempre!)

$\alpha^{-1} \equiv \alpha^6 = \alpha^2+\alpha$

$\det H^{-1} = \alpha^6$

$$H = \begin{bmatrix} \alpha^2 & \alpha^3 \\ \alpha & \alpha \end{bmatrix}$$

$$\det H = \alpha^3 - \alpha^4 = \alpha^3 + \alpha^4$$
$$= \alpha^2+1+\alpha^2+\alpha+1 = \alpha$$
$$\neq 0 \text{ OK}$$

$$H^{-1} = \alpha^6 \begin{bmatrix} \alpha & -\alpha \\ -\alpha^3 & \alpha^2 \end{bmatrix}^T =$$

$$= \alpha^6 \begin{bmatrix} \alpha & +\alpha^3 \\ +\alpha & \alpha^2 \end{bmatrix} = \begin{bmatrix} \alpha^7 & \alpha^9 \\ \alpha^7 & \alpha^8 \end{bmatrix} =$$

$$H^{-1} = \begin{bmatrix} 1 & \alpha^2 \\ 1 & \alpha \end{bmatrix}$$

α

verificare che $H \cdot H^{-1} = I$

$$\begin{bmatrix} \alpha^2 & \alpha^3 \\ \alpha & \alpha \end{bmatrix} \begin{bmatrix} 1 & \alpha^2 \\ 1 & \alpha \end{bmatrix} = \begin{bmatrix} (\alpha^2+\alpha^3) & (\alpha^4+\alpha^4=0 \\ 0 & (\alpha^2+\alpha^3) \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ OK}$$

Allora

$$c = (c_1, c_2) = (\alpha^3, \alpha) \begin{bmatrix} \alpha^2 & \alpha^3 \\ \alpha & \alpha \end{bmatrix} + (\alpha^2, \alpha^4) =$$

$$= [(\alpha^5+\alpha^2), (\alpha^6+\alpha^2)] + (\alpha^2, \alpha^4) =$$

$$= (\alpha^5+\alpha^2+\alpha^2, \ \alpha^6+\alpha^2+\alpha^4) =$$

$$= (\alpha^5, \ \cancel{\alpha^2}+\cancel{\alpha}+\cancel{\alpha^2}+\alpha^2+\cancel{\alpha}+1) = (\alpha^5, \alpha^2+1)$$

$$= (\alpha^5, \alpha^3) = (c_1, c_2) = (011, 101)$$

$$P = (C - B)\, H^{-1}$$

$$(P_1, P_2) = (\underset{\alpha+1+\alpha^2}{\alpha^5+\alpha^2}, \underset{\alpha^3+\cancel{1}+\alpha^2+\alpha+\cancel{1}}{\alpha^3+\alpha^4}) \begin{bmatrix} 1 & \alpha^2 \\ 1 & \alpha \end{bmatrix} =$$

$$= (\alpha^4, \alpha) \begin{bmatrix} 1 & \alpha^2 \\ 1 & \alpha \end{bmatrix} = (\underset{\alpha^2+\alpha+1+\alpha}{\alpha^4+\alpha}, \underset{\alpha^2+\alpha+\alpha^2}{\alpha^6+\alpha^2}) = (\alpha^3, \alpha) \text{ OK!}$$

QUESITO 4

Con lo stesso campo finito essendo $2^3-1=7=p$ ③

si assumono $P, C \in GF(2^3)(\bmod\ x^3+x^2+1)$

e $a \in \mathbb{Z}_p$; e $k \in \mathbb{Z}_p$

$1 \leq a \leq p-1$ $a \neq 0$ $k \neq 0$ $1 \leq k \leq p-1$

Ci si può applicare il crittosistema di Elgamal

ove $\beta = \alpha^a$ in $GF(2^3)$ e $C \equiv \begin{cases} r = \alpha^k \\ t = \beta^k P \end{cases}$ in $GF(2^3)(x^3+x^2+1)$

α elemento generatore essendo $g = \alpha = x$. Supponiamo $a_B = 3$

e $\beta = \alpha^3 = \alpha^2 + 1$. Alice cifra $P = \alpha^4$ con $k = 4$

$$r = \alpha^4 \ ; \quad t = (\alpha^3)^4 \alpha^4 = \alpha^{16} \equiv \alpha^2$$

$$C = (r, t) = (\alpha^4, \alpha^2)$$

Bob decifra

$$P = t r^{-a_B} \equiv \alpha^2 (\alpha^4)^{-3} = \alpha^2 \alpha^{-12} =$$

$$= \alpha^2 \alpha^{-5} \equiv \alpha^2 \alpha^2 \equiv \alpha^4 \quad \text{OK}$$

Prof. Maurizio Dècina

CRITTOGRAFIA E SICUREZZA

Secondo Appello del 25-7-2007 (due ore e quindici minuti di tempo)

Quesito 1

Alice usa il numero intero n = 6557 ($n=p\cdot q$, con p e q numeri primi) in un sistema crittografico RSA insieme alla sua chiave pubblica e=131. Oscar esegue l'**attacco di fattorizzazione di Fermat** e trova la chiave privata di Alice, d. Eseguire l'attacco:

1. Scrivere la congruenza di fattorizzazione in funzione di p e q;
2. determinare p e q;
3. determinare d.

Quesito 2

Data la congruenza $28 \equiv 2^x$ (mod 37), calcolare il logartimo discreto x = $L_2(28)$ (mod 37) con il **metodo di Pohlig-Hellman**. In particolare:

1. verificare che 2 è radice primitiva di Z_{37};
2. posto $(p - 1)= n\cdot m$, calcolare x mod n;
3. calcolare x mod m;
4. calcolare x con il teorema cinese del resto.

Data la congruenza $5 \equiv 11^x$ (mod 31), calcolare il logartimo discreto x = $L_{11}(5)$ (mod 31) applicando l'**algoritmo Baby Step Giant Step**. In particolare:

5. verificare che 11 è radice primitiva di Z_{31};
6. scegliere N, i parametri delle due liste e calcolarne i termini;
7. calcolare il logaritmo discreto x = $L_{11}(5)$.

Quesito 3

Sia date la **congruenza** $x^2 \equiv 1801$ (mod 8191), ove n = 8191 è primo di Mersenne:

1. verificare se esiste la soluzione, valutando il **simbolo di Legendre** (1801/8191).

Sia data la **congruenza** $x^2 \equiv 100$ (mod 231), ove n = 231 è composto $n = q_1q_2q_3$, con q_i primi, $1 \leq i \leq 3$.

2. Verificare che esiste la soluzione;
3. determinare i valori di x mod q_i, $1 \leq i \leq 3$;
4. calcolare x con il teorema cinese del resto.

Quesito 4

Dato il **campo finito GF**(2^3) in $\mathbf{Z}_2$[x]mod p(x), ove p(x)= x^3+ x + 1.

1. Elencare gli elementi del campo e verificare che p(x) è un *polinomio primitivo*;
2. determinare le *radici* del polinomio primitivo p(x) e verificare;
3. determinare gli *inversi* delle radici primitive;
4. indicare quanti e quali sono i *residui quadratici* del campo.

Si cifri quindi il messaggio in chiaro binario **P** = (P_1, P_2), (P_3, P_4) = (101, 010), (100, 111), con un **cifrario di Hill**: **C = P H**, e la matrice 2x2: **H** = $\begin{pmatrix} 100 & 001 \\ 011 & 001 \end{pmatrix}$, avendo numerato in binario gli elementi polinomiali del campo.

5. Quali condizioni deve rispettare la matrice **H**?
6. Determinare la matrice $\mathbf{H}^{-1}$, e verificare.
7. Qual è il messaggio cifrato binario **C**= (C_1, C_2), (C_3, C_4) ?
8. Decifrare il messaggio cifrato ottenuto al passo precedente.
9. Usando la corrispondenza tra messaggi in chiaro e messaggi cifrati ottenuta ai passi precedenti, effettuare un **attacco del tipo *known plaintext*** per ricavare la chiave **H**.

Quesito 5

Alice usa la **firma DSA** con il **gruppo ciclico** generato dalla **curva ellittica mod p**:

$$E : y^2 = x^3 + x + 6 \pmod{11}.$$

1. Determinare tutti gli elementi e l'ordine N del gruppo. Quanti e quali sono gli elementi primitivi?
2. Usare l'algoritmo *double & add* per verificare la moltiplicazione $N\cdot A=\infty$ del punto A = (2,4).
3. Identificare tutti gli elementi del gruppo ciclico generati dal punto base A = (2,4).

Alice pubblica quindi: E, p=11; q numero primo componente N, A=(2,4) e B=aA, e mantiene segreta la sua chiave a=3. Alice vuole firmare i *plaintext* m_1=3 e m_2=4 e sceglie maldestramente lo stesso *nonce* k=4.

4. Determinare le firme di Alice per i due *plaintext*: (m_1, R, s_1), (m_2, R, s_2).
5. Verificare la validità delle due firme di Alice.
6. Sfruttare l'errore di Alice con l'**attacco del nonce ripetuto,** prima per determinare il *nonce, k*, e poi:
7. per determinare la chiave segreta di Alice, a.

PUNTEGGI:

Quesito 1=2 punti; Quesito 2=4 punti; Quesito 3=6 punti; Quesito 4=9 punti; Quesito 5=9 punti.

Usare un foglio diverso per quesito con

 # Quesito, Nome, Cognome, # Matricola, Data, Firma

Quesito 4 $x^3=x+1$

000 - 0

010 - α

100 - α^2

011 - $\alpha^3=\alpha+1$

110 - $\alpha^4=\alpha^2+\alpha$

111 - $\alpha^5=\alpha^2+\alpha+1$

101 - $\alpha^6=\alpha^2+1$

001 - $\alpha^7=1$

(1) poiché $X^{2^3-1}\equiv 1 \pmod{x^3+x+1}$

x^3+x+1 è polinomio primitivo, infatti

$X^7\equiv 1 \pmod{p(x)}$

e 2^3-1 è ordine di X (esponente <u>minimo</u> per cui $X^7\equiv 1$)

(2) sono α, α^2 e α^4

$$x^3+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$$

ove $p(\alpha)=0$ infatti $\alpha^3+\alpha+1=0$

$p(\alpha^2)=0$ infatti $\alpha^6+\alpha^2+1=0$

$p(\alpha^4)=0$ infatti $\alpha^{12}+\alpha^4+1=\alpha^5+\alpha^4+1=0$

(3) le radici inverse di α, α^2 e α^4 sono: α^6, α^5 e α^3

$\alpha \to \alpha^6$ infatti $\alpha\cdot\alpha^6\equiv\alpha^7\equiv 1 \pmod{p(x)}$

$\alpha^2 \to \alpha^5$ $\qquad \alpha^2\alpha^5\equiv 1$

$\alpha^4 \to \alpha^3$ $\qquad \alpha^4\alpha^3\equiv 1$

(4) I residui quadratici sono $\frac{2^3}{2}=4$ e cioè

$\alpha^2, \alpha^4, \alpha^6, 1.$

$$H=\begin{pmatrix} 100 & 001 \\ 011 & 001 \end{pmatrix}=\begin{pmatrix} \alpha^2 & 1 \\ \alpha+1 & 1 \end{pmatrix}=\begin{pmatrix} \alpha^2 & 1 \\ \alpha^3 & 1 \end{pmatrix}$$

$$P=(101,010)(100,111)=(\alpha^2+1,\alpha)(\alpha^2,\alpha^2+\alpha+1)=(\alpha^6,\alpha),(\alpha^2,\alpha^5)$$

(5) $\det H = \alpha^2+\alpha+1=\alpha^5 \neq 0$

$\text{mcd}(\det H, p(x))=1$

p(x) è irriducibile

$\alpha^{x \bmod 7} \equiv \alpha^x$

$\alpha^{-x} \equiv \alpha^{7-x}$

(6) $(\det H)^{-1}=\dfrac{1}{\alpha^5}=(\alpha^5)^{-1}=\alpha^2$

Allora $H^{-1}=\alpha^2\begin{pmatrix} 1 & -1 \\ -(\alpha+1) & \alpha^2 \end{pmatrix}=\alpha^2\begin{pmatrix} 1 & 1 \\ \alpha+1 & \alpha^2 \end{pmatrix}=$

$$H^{-1}=\begin{pmatrix} \alpha^2 & \alpha^2 \\ \alpha^5 & \alpha^4 \end{pmatrix}=\begin{pmatrix} \alpha^2 & \alpha^2 \\ \alpha^2+\alpha+1 & \alpha^2+\alpha \end{pmatrix}$$

verifica

$$H\cdot H^{-1}=\begin{pmatrix} \alpha^2 & 1 \\ \alpha^3 & 1 \end{pmatrix}\begin{pmatrix} \alpha^2 & \alpha^2 \\ \alpha^5 & \alpha^4 \end{pmatrix}=$$

$$=\begin{pmatrix} \alpha^4+\alpha^5 & \alpha^4+\alpha^4 \\ \alpha^5+\alpha^5 & \alpha^5+\alpha^4 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I$$

ok

(7) $(C_1,C_2)=(P_1\ P_2)H=$

$$=(\alpha^6,\alpha)\begin{pmatrix}\alpha^2 & 1\\ \alpha^3 & 1\end{pmatrix}=(\alpha^8+\alpha^4),(\alpha^6+\alpha)=$$

$$=(\alpha^2,\alpha^5)=(\alpha^2,\alpha^2+\alpha+1)$$

$C_1=\alpha^2=100$

$C_2=\alpha^2+\alpha+1=111$

$(C_3,C_4)=(P_3,P_4)H=$

$$=(\alpha^2,\alpha^5)\begin{pmatrix}\alpha 2 & 1\\ \alpha 3 & 1\end{pmatrix}=(\alpha^4+\alpha^8),(\alpha^2+\alpha^5)=$$

$$=(\alpha^2,\alpha^3)=(\alpha^2,\alpha+1)$$

$C_3=\alpha^2=100$

$C_4=\alpha+1=011$

(8)

$(P_3,P_4)=(C_3,C_4)H^{-1}=$

$$=(\alpha^2,\alpha^3)\begin{pmatrix}\alpha^2 & \alpha 2\\ \alpha 5 & \alpha 4\end{pmatrix}=(\alpha^4+\alpha^8),(\alpha^4+\alpha^7)=$$

$$=(\alpha^2,\alpha^5)=(\alpha^2,\alpha^2+\alpha+1)$$

$P_3=\alpha 4$

$P_4=\alpha 5$

ok

$(P_1,P_2)=(C_1,C_2)H^{-1}=$

$$=(\alpha^2,\alpha^5)\begin{pmatrix}\alpha 2 & \alpha 2\\ \alpha 5 & \alpha^4\end{pmatrix}=(\alpha^4+\alpha^{10}),(\alpha^4+\alpha^9)=$$

$$=(\alpha^4+\alpha^3),(\alpha^4+\alpha^2)=(\alpha_6,\alpha)$$

$P_1=\alpha^6$, $P_2=\alpha$ ok

(g) $\begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} H = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$

deve essere $\det \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} \neq 0$ $\quad \det \underline{P} \neq 0$

$$\det \begin{pmatrix} \alpha^6 & \alpha \\ \alpha^2 & \alpha^5 \end{pmatrix} = \alpha^6 \alpha^5 - \alpha^3 = \alpha^{11} + \alpha^3 =$$

$$= \alpha^4 + \alpha^3 = \alpha^6 = \alpha^2 + 1 \neq 0$$

Allora

$$H = \begin{pmatrix} \alpha^6 & \alpha \\ \alpha^2 & \alpha^5 \end{pmatrix}^{-1} \begin{pmatrix} \alpha^2 & \alpha^5 \\ \alpha^2 & \alpha^3 \end{pmatrix} =$$

ma

$$= \begin{pmatrix} \alpha^6 & \alpha \\ \alpha^2 & \alpha^5 \end{pmatrix}^{-1} = (\det \underline{P})^{-1} \begin{pmatrix} \alpha^5 & -\alpha^2 \\ -\alpha & \alpha^6 \end{pmatrix}^T =$$

$$= \alpha \cdot \begin{pmatrix} \alpha^5 & -\alpha \\ -\alpha^2 & \alpha^6 \end{pmatrix} = \begin{pmatrix} \alpha^6 & \alpha^2 \\ \alpha^3 & 1 \end{pmatrix}$$

allora

$$H = \begin{pmatrix} \alpha^6 & \alpha^2 \\ \alpha^3 & 1 \end{pmatrix} \begin{pmatrix} \alpha^2 & \alpha^5 \\ \alpha^2 & \alpha^3 \end{pmatrix} = \begin{pmatrix} \alpha^8 + \alpha^4 & \alpha^{11} + \alpha^5 \\ \alpha^5 + \alpha^2 & \alpha^8 + \alpha^3 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^2 & 1 \\ \alpha^3 & 1 \end{pmatrix}.$$ ok!

Prof. Maurizio Dècina

CRITTOGRAFIA E SICUREZZA

Terzo Appello del 10-9-2007 (due ore e quindici minuti di tempo)

Quesito 1

Verificare se il numero intero n = 341 è primo utilizzando i tre **test di Fermat**, **di Miller-Rabin e di Solovay-Strassen,** con basi a = 2 e a = 3.

1. Test di Fermat.
2. Test di Miller-Rabin.
3. Test di Solovay-Strassen.

Quesito 2

Data la congruenza $12 \equiv 7^x \pmod{41}$, calcolare il logartmo discreto $x = L_7(12) \pmod{41}$ con il **metodo di Pohlig-Hellman**. In particolare:

1. verificare che 7 è *radice primitiva* di Z_{41};
2. posto $(p - 1)= n\cdot m$, calcolare x mod n;
3. calcolare x mod m;
4. calcolare x con il *teorema cinese del resto*.

Quesito 3

Alice usa il numero intero n = 1.961 ($n=p\cdot q$, con p e q primi) in un **sistema crittografico RSA** insieme alla sua chiave pubblica e=11. Oscar esegue l'**attacco di fattorizzazione con *l'algoritmo p-1***, utilizzando la base a=2 e il *bound* B=7, e trova la chiave privata di Alice, d. Eseguire l'attacco:

1. determinare i coefficienti b_i, $1\leq i \leq 7$;
2. verificare il valore di b_7;
3. determinare p e q;
4. determinare d.

Quesito 4

Si consideri un testo in chiaro composto dalle 26 lettere maiuscole dell'alfabeto inglese, numerate da 65 a 90. Alice e Bob usano il **crittosistema di Rabin** e adottano come chiave pubblica n=209 e come chiave privata segreta la fattorizzazione $n=p\cdot q = 19 \cdot 11$. Alice cifra a caratteri isolati (ECB) il messaggio in chiaro P_1= D= 68; P_2= E=69, e lo invia a Bob.

1. Con quali interi, C_1, C_2 mod n, Alice cifra il messaggio in chiaro, P_1, P_2?
2. Come decifra Bob il messaggio cifrato C_1 inviato da Alice?
3. Come decifra Bob il messaggio cifrato C_2 inviato da Alice?
4. Oscar effettua un **attacco *chosen chiphertext*** basato su C_1 e ha a disposizione il decifratore di Alice per alcune prove; in corrispondenza di C_1 il decifratore restituisce due *plaintext:* P_1mod209 e $P_x$mod209, tali che risulta $\pm P_1 \neq \pm P_x$ (mod209); come fa Oscar a determinare la chiave privata e quindi a decifrare C_2?

Quesito 5

Dato il **campo finito GF**(2^4) in $\mathbf{Z}_2[x]$mod p(x), ove $p(x)= x^4+ x^3 + 1$.

1. Elencare gli elementi del campo;
2. verificare che p(x) è un *polinomio primitivo*;
3. determinare le *radici* del polinomio primitivo p(x) e verificare;
4. determinare gli *inversi* delle radici primitive;
5. indicare quanti e quali sono i *residui quadratici* del campo.

Realizzare un **crittosistema di ElGamal**, assumendo che: $P,C \in GF(2^4)$ (mod $x^4+ x^3 + 1$), mentre il segreto, a, di Bob e il nonce, k, di Alice sono numeri interi: $1 \leq a, k \leq (2^4-2)$. Come radice primitiva del campo ciclico si utilizza $x = \alpha$ = 0010. La chiave pubblica di Bob è $\beta = \alpha^a$. Bob pubblica: [$GF(2^4)$ (mod $x^4+ x^3 + 1$), α, β] e tiene segreta la sua chiave a=7. Alice sceglie il nonce k = 5 e cifra il testo in chiaro P = 1111.

6. Qual'è il testo cifrato C = (r, t), ove $r, t \in GF(2^4)$ (mod $x^4+ x^3 + 1$)?
7. Come decifra Bob il messaggio ricevuto C = (r, t)?

Quesito 6

Alice usa la **firma ElGamal** con il **gruppo ciclico** generato dalla **curva ellittica mod p**:

$$E : y^2 = x^3 + 2x + 1 \pmod{11}.$$

1. Verificare la *non singolarità* della curva.
2. Usare i *simboli di Legendre* e le *formule per radici quadrate* per determinare tutti gli elementi e l'ordine N del gruppo.
3. Usare l'algoritmo *double & add* per verificare la moltiplicazione $N\cdot A=\infty$ del punto A = (5,2).
4. Quanti e quali sono gli *elementi primitivi*?
5. Identificare tutti gli elementi del gruppo ciclico generati dal **punto base** A = (5,2).

Alice pubblica: [E, p=11, N, A=(5,2), B=aA] e mantiene segreta la sua chiave a=4.

Alice vuole firmare il messaggio in chiaro m =3 ($0 \leq m \leq N -1$) e sceglie il *nonce* k=5, essendo mcd (k,N)=1.

6. Determinare la firma di Alice: (m, R, s).
7. Verificare la validità della firma di Alice.

PUNTEGGI:

Quesito 1=3 punti; Quesito 2=4 punti; Quesito 3=4 punti;

Quesito 4=5 punti; Quesito 5=7 punti; Quesito 6=7punti.

Usare un foglio diverso per quesito con: # Quesito, Nome, Cognome, # Matricola, Data, Firma

Quesito4

$n = 209 = p \cdot q$ $\quad (A \div Z) \equiv (65 \div 90)$ mod 209

$p = 11 ; q = 19$

cifratura di Rabin $\quad P = (68, 69) \rightarrow P_1 = 68 ; P_2 = 69$

- $$C_i = P_i^2 \bmod 209 \longrightarrow \begin{cases} c_1 = 26 \\ c_2 = 163 \end{cases} (\bmod 209)$$

- Decifriamo $c_1 = 26$ conoscendo $p = 11$ e $q = 19$ $(p \cdot q = n)$

si ha che $\quad x^2 \equiv 26 \pmod{209}$

$$\begin{cases} a_1^2 = 26 \bmod 11 = 4 \\ a_2^2 = 26 \bmod 19 = 7 \end{cases}$$

$$\begin{cases} a_1 = 4^{\frac{11+1}{4}} \bmod 11 \equiv 4^3 \equiv 9 \pmod{11} \\ a_2 \equiv 7^{\frac{19+1}{4}} \equiv 7^5 \equiv 11 \pmod{19} \end{cases}$$

radici quadrate $\pm a_1 \equiv \pm 9 \pmod{11}$

$\pm a_2 \equiv \pm 11 \pmod{19}$

$z_1 = 19 ; z_2 = 11$

$y_1 = 19^{-1} \bmod 11 \equiv 19^{10} \equiv 7 \bmod 11$

$y_2 = 11^{-1} \bmod 19 = 11^{17} \equiv 7 \bmod 19$

$$X = \sum_i (\pm a_i) \, y_i \, z_i \pmod{n}$$

$$X=\begin{cases} 9\cdot19\cdot7+11\cdot11\cdot7\equiv163\\ 9\cdot19\cdot7-11\cdot11\cdot7\equiv141\\ -9\cdot19\cdot7+11\cdot11\cdot7\equiv68\\ -9\cdot19\cdot7-11\cdot11\cdot7\equiv46\end{cases} \pmod{209}$$

Bob sceglie $X=68\equiv D$ e scarta tutte le altre OK.

• Decifriamo $C_2=163$ $\quad x^2\equiv163 \pmod{209}$

si ha che

$$\begin{cases} a_1^2=163 \bmod 11=9\\ a_2^2=163 \bmod 19=11\end{cases} \qquad \begin{cases} a_1\equiv9^3\equiv3 \pmod{11}\\ a_2\equiv11^5\equiv7 \pmod{19}\end{cases}$$

$$x=\sum_i(\pm a_1)y_i z_i \pmod n$$

$$X=\begin{cases} 3\cdot19\cdot7+7\cdot11\cdot7\equiv102\\ 3\cdot19\cdot7-7\cdot11\cdot7\equiv69\\ -3\cdot19\cdot7+7\cdot11\cdot7\equiv140\\ -3\cdot19\cdot7-7\cdot11\cdot7\equiv107\end{cases} \pmod{209}$$

Bob sceglie $X=69\equiv E$ e scarta le altre OK.

• Oscar ha $C_1=26 \bmod 209$ e non conosce $n=p\cdot q$, e cioè $p=11$ e $q=19$. Oscar immette C_1 nel decifratore di Alice e ricava, ad esempio, due diversi plaintext: 68 e 46. Verifica che $\pm68\neq\pm46 \pmod{209}$ e applica la formula

$\mathrm{mcd}(68-46, 209) =$

$\mathrm{mcd}(22, 209) = (11, 22) = (0, 11) = 11 = p$

BINGO!

Oscar calcola quindi $\frac{n}{p} = q = \frac{209}{11} = 19$,

e quindi può ora agevolmente decifrare C_2.

NB. Si suppone che Oscar conosca il range (65÷90) adot~~tato~~ per le 26 lettere inglesi

---

Quesito 5

$GF(2^4)$ in $\mathbb{Z}_2[x] \pmod{x^4+x^3+1}$

$p(x) = 0$ per $x_i = \alpha^{2^{i-1}}$, $1 \le i \le 4$

1. Residui 0

$\boxed{\alpha^4 = \alpha^3 + 1}$ $(\mathrm{mod}\ \alpha^4+\alpha^3+1)$

0010 - α
0100 - α^2
1000 - α^3
1001 - $\alpha^4 = \alpha^3+1$
- $\alpha^5 = \alpha^3+\alpha+1$
- $\alpha^6 = \alpha^3+\alpha^2+\alpha+1$
- $\alpha^7 = \alpha^2+\alpha+1$
$\alpha^8 = \alpha^3+\alpha^2+\alpha$
$\alpha^9 = \alpha^2+1$
$\alpha^{10} = \alpha^3+\alpha$
$\alpha^{11} = \alpha^3+\alpha^2+1$
$\alpha^{12} = \alpha+1$
$\alpha^{13} = \alpha^2+\alpha$
$\alpha^{14} = \alpha^3+\alpha^2$
0001 - $\alpha^{15} = 1$

2. per verificare che $p(x)$ è primitivo va verificato che l'ordine di $x = \alpha$ è 2^4-1 è cioè 15 è il minimo esponente di α tale che $\alpha^k \equiv 1 \pmod{p(x)}$

ok!

$\alpha^k \equiv \alpha^{k \bmod 15}$ per $k > 15$

3. $p(X)=0$ per $X_i=\alpha^{2^{i-1}}$ per $i=1,2,3,4$

4 radici: $X=\alpha;\ \alpha^2;\ \alpha^4;\ \alpha^8$

verifica

$$p(X)=(X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8);$$ infatti

$$p(X)=\prod_{i=0}^{m-1}(X-\alpha^{2^i})$$ per $m=4$ grado del polinomio

si ha $p(X)=(X^2+X(\alpha^2+\alpha)+\alpha^3)(X^2+X(\alpha^8+\alpha^4)+\alpha^{12})=$

$=(X^2+X\alpha^{13}+\alpha^3)(X^2+X\alpha^7+\alpha^{12})=$

$=X^4+X^3\alpha^7+X^2\alpha^{12}+X^3\alpha^{13}+X^2\alpha^{20}+X\alpha^{25}+X^2\alpha^3+$

$+X\alpha^{10}+\alpha^{15}=X^4+X^3(\alpha^7+\alpha^{13})+X^2(\alpha^{12}+\alpha^{20}+\alpha^3)+$

$+X(\alpha^{25}+\alpha^{10})+\alpha^{15}=$

$=X^4+X^3+X^2(0)+X(0)+1=X^4+X^3+1$ ok

4. gli inversi delle radici di $p(X)$ sono

X	X^{-1}
α	α^{14}
α^2	α^{13}
α^4	α^{11}
α^8	α^7

avendo $X\cdot X^{-1}\equiv 1\ (\mathrm{mod}\ pX)$

5. I residui quadratici sono 8 (esponenti pari +1)

RQ: $\alpha^2;\ \alpha^4;\ \alpha^6;\ \alpha^8;\ \alpha^{10};\ \alpha^{12};\ \alpha^{14};\ \alpha^{15}\equiv 1$

Radici dei residui quadratici $\pm\alpha;\ \pm\alpha^2;\ \pm\alpha^3;\ \pm\alpha^4;\ \pm\alpha^5;\ \pm\alpha^6;\ \pm\alpha^7;\ \pm 1$

6. Campo finito $2^4-1=15$

$$P, C \in GF(2^4)(\bmod x^3+x^2+1)$$

$a, k \in \mathbb{Z}_{15}$; $a, k \neq 0$ $\quad 1 \leq a, k \leq 14$

$$\beta = \alpha^a \qquad C = \begin{cases} r = \alpha^k \\ t = \beta^k P \end{cases} \text{ in } GF(2^4)(\bmod px)$$

α elemento generatore $\quad \alpha = x = 0010$; $a = 7$

$\beta = \alpha^7 = \alpha^2+\alpha+1$. Alice cifra $P = 1111 = \alpha^6 =$
$= \alpha^3+\alpha^2+\alpha+1$
con $k=5$

$$\begin{cases} r = \alpha^5 \\ t = (\alpha^7)^5 \alpha^6 = \alpha^{41} = \alpha^{11} \end{cases}$$

$$P = \alpha^6 \rightarrow C = (r, t) = (\alpha^5, \alpha^{11})$$

7. Bob decifra

$$P = t\, r^{-a} = \alpha^{11} \cdot (\alpha^5)^{-7} = \alpha^{11} \alpha^{-35} =$$

$$= \alpha^{11} \alpha^{-5} = \alpha^{11} \alpha^{10} = \alpha^{21} = \alpha^6 \text{ OK}$$

Prof. Maurizio Dècina

CRITTOGRAFIA E SICUREZZA

Quarto Appello del 24-9-2007 (due ore e quindici minuti di tempo)

Quesito 1

Data la congruenza $11\equiv 2^x$ (mod 13), calcolare il logaritmo discreto $x=L_2(11)$ con il **metodo di Pohlig-Hellman**. In particolare:

1. verificare che 2 è radice primitiva di Z_{13};
2. posto $(p-1)= n\cdot m$, calcolare x mod n;
3. calcolare x mod m;
4. calcolare x con il teorema cinese del resto.

Data la congruenza $27\equiv 5^x$ (mod 103), calcolare il logartimo discreto $x=L_5(27)$ (mod 103) applicando l'**algoritmo Baby Step Giant Step**. In particolare:

5. verificare che 5 è radice primitiva di Z_{103};
6. scegliere N, i parametri delle due liste e calcolarne i termini;
7. calcolare il logaritmo discreto $x=L_5(27)$.

Calcolare lo stesso logartimo discreto $x=L_5(27)$ (mod 103) applicando l'**algoritmo Index Calculus**. Scegliere il *bound* B=8 per la *base di fattori* primi: [2, 3, 5, 7], $p_i \le B$ $(1\le i \le 4)$. In particolare:

8. esprimere le potenze di 5^k come prodotto di elementi della base di fattori *(provare per* $1\le k \le 11$*)* ;
9. determinare i valori dei logaritmi discreti $L_5(p_i)$ per i fattori p_i =2, 3, 5, 7;
10. determinare il logaritmo discreto $x=L_5(27)$.

Quesito 2

Dato il **campo finito GF**(2^4) in $\mathbf{Z}_2[x]$mod p(x), ove $p(x)= x^4+ x + 1$.

1. Elencare tutti gli elementi del campo e verificare che p(x) è un *polinomio primitivo*;
2. determinare le *radici* del polinomio primitivo p(x) e verificare;
3. Quanti e quali sono gli *elementi primitivi* del campo?
4. Indicare quanti e quali sono i *residui quadratici* del campo;
5. determinare *l'ordine di ciascuno degli elementi* del campo.

Si cifri quindi il messaggio in chiaro binario **P**= (P_1, P_2), (P_3, P_4)=(0101, 0010), (0100, 1111), con un **cifrario di Hill**: **C = P H**, e la matrice 2x2: **H** = $\begin{pmatrix}1000 & 0001\\ 1111 & 0001\end{pmatrix}$, avendo numerato in binario gli elementi polinomiali del campo.

6. Quali condizioni deve rispettare la matrice **H**? Determinare la matrice $\mathbf{H}^{-1}$, e verificare.
7. Quale è il messaggio cifrato binario **C**= (C_1, C_2), (C_3, C_4)?
8. Decifrare il messaggio cifrato ottenuto al passo precedente.
9. Usando la corrispondenza tra messaggi in chiaro e messaggi cifrati ottenuta ai passi precedenti, effettuare un **attacco del tipo *known plaintext*** per ricavare la chiave **H**.

Si realizzi poi un **crittosistema di ElGamal**, assumendo che: $P,C\in GF(2^4)$mod p(x), mentre il segreto, a, di Bob e il *nonce*, k, di Alice sono numeri interi: $1 \le a, k \le (2^4-2)$. Come *radice primitiva* del campo si utilizza $x=\alpha$= 0010. La chiave pubblica di Bob è $\beta=\alpha^a$. Bob pubblica: $[GF(2^4)$mod p(x), α, β] e tiene segreta la sua chiave a=3. Alice sceglie il *nonce* k = 4 e cifra il testo in chiaro P= 1111.

10. Quale è il testo cifrato C = (r, t), ove r, t $\in GF(2^4)$mod p(x)?
11. Come decifra Bob il messaggio ricevuto C= (r, t)?

Quesito 3

Alice usa la **firma ElGamal** con il **gruppo ciclico** generato dalla **curva ellittica mod p**:

$$E : y^2 = x^3 + 3 \pmod{11}.$$

1. Verificare la *non singolarità* della curva.
2. Usare i *simboli di Legendre* e le *formule per radici quadrate* per determinare tutti gli elementi e l'ordine N del gruppo.
3. Usare l'algoritmo *double & add* per verificare la moltiplicazione $N\cdot A=\infty$ del punto A= (4,1).
4. Identificare tutti gli elementi del gruppo ciclico generati dal **punto base** A= (4,1).
5. Quanti e quali sono gli *elementi primitivi*?
6. Determinare *l'ordine di ciascuno degli elementi del gruppo*.

Effettuare poi un parallelismo con il **campo finito** Z^*_q, ove $q=N+1$.

7. Quanti e quali sono gli *elementi primitivi* di Z^*_q= [*1, 2, 3...., N-1, N*]?
8. Determinare *l'ordine di ciascuno degli elementi* di Z^*_q.

Alice pubblica quindi: [E, *p*=11, N, A=(4,1), B=*a*A], e mantiene segreta la sua chiave *a*=3. Alice vuole firmare i *plaintext* m_1=3 e m_2=5 e sceglie maldestramente lo stesso *nonce* *k*=5.

9. Determinare le firme di Alice per i due *plaintext*: (m_1, R, s_1), (m_2, R, s_2).
10. Verificare la validità delle due firme di Alice.
11. Sfruttare l'errore di Alice con l'**attacco del nonce ripetuto,** per determinare il *nonce, k*, e la chiave segreta di Alice, *a*.

PUNTEGGI: Quesito 1=8 punti; Quesito 2=11 punti; Quesito 3=11 punti;

Usare un foglio diverso per quesito con: # Quesito, Nome, Cognome, # Matricola, Data, Firma

QUESITO 2

$\alpha^4 \equiv \alpha + 1 \pmod{\alpha^4+\alpha+1}$

⑥

① gli elementi di $GF(2^4) \pmod{x^4+x+1}$ sono

$0000 - 0$
$0010 - \alpha$
$0100 - \alpha^2$
$1000 - \alpha^3$
$0011 - \alpha^4 = \alpha+1$
$0110 - \alpha^5 = \alpha^2+\alpha$
$1100 - \alpha^6 = \alpha^3+\alpha^2$
$1011 - \alpha^7 = \alpha^3+\alpha+1$ $\quad \pmod{\alpha^4+\alpha+1}$
$0101 - \alpha^8 = \alpha^2+1$
$1010 - \alpha^9 = \alpha^3+\alpha$
$0111 - \alpha^{10} = \alpha^2+\alpha+1$
$1110 - \alpha^{11} = \alpha^3+\alpha^2+\alpha$
$1111 - \alpha^{12} = \alpha^3+\alpha^2+\alpha+1$
$1101 - \alpha^{13} = \alpha^3+\alpha^2+1$
$1001 - \alpha^{14} = \alpha^3+1$
$0001 - \alpha^{15} = 1$

$p(x) = x^4+x+1$ è primitivo perchè l'ordine dell'elemento $x=\alpha$ è $2^4-1=15$

② $2^4-1=15=3\cdot 5$ mcd $(i,15)=1$ per $i = 7, 11, 13, 14$ e per $i = 1, 2, 4, 8 \rightarrow i = 2^k \quad 0 \le k \le n-1 \quad (n=4)$

allora le radici $p(x)=0$ sono $\{\alpha, \alpha^2, \alpha^4, \alpha^8\} \pmod{\alpha^4+\alpha+1}$

7 verifichiamo che $p(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$ ⑦

$$= x^4+x+1 \pmod{x^4+x+1}$$

infatti

$$p(x)=(x^2+x\alpha^5+\alpha^3)\left[(x^2+x\alpha^5+\alpha^3)+\alpha^{10}\right]=$$

$$=(x^2+x\alpha^5+\alpha^3)^2+(x^2+x\alpha^5+\alpha^3)\alpha^{10}=$$

$$=(x^4+x^2\alpha^{10}+\alpha^6)+(x^2\alpha^{10}+x\alpha^{15}+\alpha^{13})=$$

$$=x^4+x+\alpha^6+\alpha^{13}=x^4+x+1 \quad \text{ok}$$

③

$\varphi(2^4-1)=\varphi(3\cdot 5)=8$

gli elementi primitivi sono le radici di $p(x)=x4+x+1$, α,α^2,α^4 e α^8 e i loro inversi: $\alpha^{14},\alpha^{13},\alpha^{11},\alpha^7$,

(radici di $p_2(x)=x^4+x^3+1$) tutti

tali $\text{mcd}(i,15)=1$.

④ i residui quadratici sono quelli per cui α^i $1\leq i\leq 15$ $(\text{mod } \alpha^4+\alpha+1)$

ove i è pari $(\alpha^2,\alpha^4,\alpha^6,\alpha^8,\alpha^{10},\alpha^{12},\alpha^{14})$

e in più c'è l'unità $\alpha^{15}\equiv 1$.

Sono $2^4/2=8$.

⑤ L'ordine degli 8 elementi primitivi è 15: ⑧

$$\{\alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}, \alpha^{14}\} \text{ ORD} = 15$$

verifichiamo ad esempio α^2

$(\alpha^2)^i$	α^4	α^6	α^8	α^{10}	α^{12}	α^{14}	α	α^3	α^5	α^7	α^9	α^{11}	α^{13}	1
i	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Cerchiamo poi $\text{ORD} = \frac{2^4-1}{3} = 5$ e $\text{ORD} = \frac{2^4-1}{5} = 3$

e verifichiamo

$$(\alpha^3)^i \to (\alpha^3)^3 \equiv \alpha^9 \to (\alpha^3)^5 \equiv \alpha^{15} \equiv 1 \to \text{ORD} = 5$$

$$(\alpha^5)^i \to (\alpha^5)^3 \equiv 1 \quad \text{ORD} = 3$$

$$(\alpha^6)^i \to (\alpha^6)^3 \equiv \alpha^3 \to (\alpha^3)^5 \equiv 1 \to \text{ORD } 5$$

Questi ordini sono gli stessi degli <u>inversi</u>

$$\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\} \text{ ORD } 5$$

$$\{\alpha^5, \alpha^{10}\} \text{ ORD } 3$$

⑥ $H \equiv \begin{pmatrix} \alpha^3 & 1 \\ \alpha^{12} & 1 \end{pmatrix}$

$\det H = \alpha^3 + \alpha^{12} = \alpha^3 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha + 1 = \alpha^{10}$

$\det H \neq 0$ ok

$\det H^{-1} = (\alpha^{10})^{-1} = \alpha^5$

$H^{-1} = \alpha^5 \begin{pmatrix} 1 & 1 \\ \alpha^{12} & \alpha^3 \end{pmatrix} = \begin{pmatrix} \alpha^5 & \alpha^5 \\ \alpha^2 & \alpha^8 \end{pmatrix}$

$H \cdot H^{-1} = \begin{pmatrix} \alpha^3 & 1 \\ \alpha^{12} & 1 \end{pmatrix} \begin{pmatrix} \alpha^5 & \alpha^5 \\ \alpha^2 & \alpha^8 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

infatti $\alpha^3 \cdot \alpha^5 + \alpha^2 = \alpha^8 + \alpha^2 = 1$

$\alpha^3 \cdot \alpha^5 + \alpha^8 = \alpha^8 + \alpha^8 = 0$

$\alpha^{12} \cdot \alpha^5 + \alpha^2 = \alpha^2 + \alpha^2 = 0$

$\alpha^{12} \alpha^5 + \alpha^8 = \alpha^2 + \alpha^2 + 1 = 1$

⑦ ciphering

$C = P \cdot H = \begin{pmatrix} \alpha^8 & \alpha \\ \alpha^2 & \alpha^{12} \end{pmatrix} \begin{pmatrix} \alpha^3 & 1 \\ \alpha^{12} & 1 \end{pmatrix} = \begin{pmatrix} \alpha^4 & \alpha^{10} \\ \alpha^{16} & \alpha^7 \end{pmatrix}$

$\det P = \alpha^8 \alpha^{12} + \alpha^3 = \alpha^5 + \alpha^3 = \alpha^3 + \alpha^2 + \alpha = \alpha^{11} \neq 0$

verifichiamo C $\alpha^8 \cdot \alpha^3 + \alpha \cdot \alpha^{12} = \alpha^{11} + \alpha^{13} = \alpha + 1 = \alpha^4$

$\alpha^8 + \alpha = \alpha^2 + \alpha + 1 = \alpha^{10}$

$$\alpha^5+\alpha^{24}=\alpha^5+\alpha^9=\alpha^3+\alpha^2=\alpha^6$$

$\det C=\alpha^{17}+\alpha^{16}=\alpha^2+1\neq 0$ $\quad \alpha^2+\alpha^{12}=\alpha^3+\alpha+1=\alpha^7$

quindi

$$P=(\alpha^8,\alpha)(\alpha^2,\alpha^{12})=(0101,0010)(0100,1111)$$

$$C=(\alpha^4,\alpha^{10})(\alpha^6,\alpha^7)=(0011,0111)(1100,1011)$$

⑧ Deciphering

$$P=CH^{-1}=\begin{pmatrix}\alpha^4 & \alpha^{10}\\ \alpha^6 & \alpha^7\end{pmatrix}\begin{pmatrix}\alpha^5 & \alpha^5\\ \alpha^2 & \alpha^8\end{pmatrix}=\begin{pmatrix}\alpha^8 & \alpha\\ \alpha^2 & \alpha^{12}\end{pmatrix}$$

infatti

$$\alpha^4\cdot\alpha^5+\alpha^{10}\alpha^2=\alpha^9+\alpha^{12}=\alpha^2+1=\alpha^8$$

$$\alpha^9+\alpha^{18}=\alpha^9+\alpha^3=\alpha$$

$$\alpha^{11}+\alpha^9=\alpha^2$$

$$\alpha^{11}+\alpha^{15}=\alpha^3+\alpha^2+\alpha+1=\alpha^{12}$$

⑨ Attacco Known Plaintext

$P=\begin{pmatrix}\alpha^8 & \alpha\\ \alpha^2 & \alpha^{12}\end{pmatrix}$ $\quad \det P=\alpha^{11}$ $\quad \det P^{-1}=\alpha^4=\alpha+1$

$$P^{-1}=\alpha^4\begin{pmatrix}\alpha^{12} & \alpha\\ \alpha^2 & \alpha^8\end{pmatrix}=\begin{pmatrix}\alpha & \alpha^5\\ \alpha^6 & \alpha^{12}\end{pmatrix}$$

verifico

$$P\cdot P^{-1}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}\alpha^8 & \alpha\\ \alpha^2 & \alpha^{12}\end{pmatrix}\begin{pmatrix}\alpha & \alpha^5\\ \alpha^6 & \alpha^{12}\end{pmatrix}$$

$\alpha^8\cdot\alpha+\alpha\alpha^6=\alpha^9+\alpha^7=1;$ $\quad \alpha^{13}+\alpha^{13}=0$

$\alpha^3+\alpha^{18}=\alpha^3+\alpha^3=0$ $\quad \alpha^7+\alpha^{24}=\alpha^7+\alpha^9=1$

$$H = P^{-1}C = \begin{pmatrix}\alpha & \alpha^5\\ \alpha^6 & \alpha^{12}\end{pmatrix}\begin{pmatrix}\alpha^4 & \alpha^{10}\\ \alpha^6 & \alpha^7\end{pmatrix} = \begin{pmatrix}\alpha^3 & 1\\ \alpha^{12} & 1\end{pmatrix}$$

BINGO!

$\alpha\cdot\alpha^4+\alpha^5\cdot\alpha^6=\alpha^5+\alpha^{11}=\alpha^3$

$\alpha^{11}+\alpha^{12}=1$

$\alpha^{10}+\alpha^{18}=\alpha^{10}+\alpha^3=\alpha^{12}$

$\alpha^{16}+\alpha^{19}=\alpha+\alpha^4=1$

OK!

---

⑩ ElGamal cryptosysten

$P=\alpha^{12}$ $\beta=\alpha^a=\alpha^3$ $a_B=3$

ciphering

$$\begin{cases} r=\alpha^{k_A}=\alpha^4 \\ t=(\alpha^3)^4\alpha^{12}=\alpha^{24}=\alpha^9=\beta^{k_A}P\end{cases}$$

$k_A=4$

$$C=(r,t)=(\alpha^4,\alpha^9)$$

⑪ deciphering

$$P=t\,r^{-a_B}=\alpha^9(\alpha^4)^{-3}=\alpha^9\alpha^{-12}=$$

$$=\alpha^9\alpha^3=\alpha^{12}$$

OK!

Prof. Maurizio Dècina

CRITTOGRAFIA E SICUREZZA

Qinto Appello del 11-2-2008 (due ore di tempo)

Quesito 1

Sia date la **congruenza** $x^2 \equiv 1801 \pmod{8191}$, ove n = 8191 è primo di Mersenne:

1. verificare se esiste la soluzione, valutando il **simbolo di Legendre** (1801/8191).

Sia data la **congruenza** $x^2 \equiv 100 \pmod{231}$, ove n = 231 è composto $n = q_1 q_2 q_3$, con q_i primi, $1 \le i \le 3$.

2. Verificare che esiste la soluzione;
3. determinare i valori di x mod q_i, $1 \le i \le 3$;
4. calcolare x con il *teorema cinese del resto*.

Quesito 2

Data la congruenza $12 \equiv 7^x \pmod{41}$, calcolare il logaritmo discreto $x = L_7(12) \pmod{41}$ con il **metodo di Pohlig-Hellman**. In particolare:

1. verificare che 7 è *radice primitiva* di Z_{41};
2. posto $(p-1) = n \cdot m$, calcolare x mod n;
3. calcolare x mod m;
4. calcolare x con il *teorema cinese del resto*.

Quesito 3

Dato il **campo finito GF**(2^3) in $\mathbf{Z}_2[x]$mod p(x), ove $p(x) = x^3 + x + 1$.

1. Elencare gli elementi del campo e verificare che p(x) è un *polinomio primitivo*;
2. determinare le *radici* del polinomio primitivo p(x) e verificare;
3. determinare gli *inversi* delle radici primitive;
4. indicare quanti e quali sono i *residui quadratici* del campo.

Si cifri quindi il messaggio in chiaro binario **P** = $(P_1, P_2), (P_3, P_4)$ = (101, 010), (100, 111), con un **cifrario di Hill**:

C = P H, e la matrice 2x2: **H** = $\begin{pmatrix} 100 & 001 \\ 011 & 001 \end{pmatrix}$, avendo numerato in binario gli elementi polinomiali del campo.

5. Quali condizioni deve rispettare la matrice **H**?
6. Determinare la matrice $\mathbf{H}^{-1}$, e verificare.
7. Qual è il messaggio cifrato binario **C**= $(C_1, C_2), (C_3, C_4)$?
8. Decifrare il messaggio cifrato ottenuto al passo precedente.
9. Usando la corrispondenza tra messaggi in chiaro e messaggi cifrati ottenuta ai passi precedenti, effettuare un **attacco del tipo *known plaintext*** per ricavare la chiave **H**.

Quesito 4

Alice usa la **firma ElGamal** con il **gruppo ciclico** generato dalla **curva ellittica mod p**:

$$E : y^2 = x^3 + 2x + 1 \pmod{11}.$$

1. Verificare la *non singolarità* della curva.
2. Usare i *simboli di Legendre* e le *formule per radici quadrate* per determinare tutti gli elementi e l'ordine N del gruppo.
3. Usare l'algoritmo *double & add* per verificare la moltiplicazione $N \cdot A = \infty$ del punto A = (5,2).
4. Quanti e quali sono gli *elementi primitivi*?
5. Identificare tutti gli elementi del gruppo ciclico generati dal **punto base** A = (5,2).

Alice pubblica: [E, *p*=11, N, A=(5,2), B=*a*A] e mantiene segreta la sua chiave *a*=4.

Alice vuole firmare il messaggio in chiaro *m* =3 $(0 \le m \le N-1)$ e sceglie il *nonce* *k*=5, essendo mcd (k,N)=1.

6. Determinare la firma di Alice: (*m*, R, *s*).
7. Verificare la validità della firma di Alice.

PUNTEGGI: Quesito 1=6 punti; Quesito 2=6 punti; Quesito 3 =10 punti; Quesito 4=8 punti.

Usare un foglio diverso per quesito con: # Quesito, Nome, Cognome, # Matricola, Data, Firma

Quesito 4 $x^3=x+1$ ①

000 - 0
010 - α
100 - α^2
011 - $\alpha^3=\alpha+1$
110 - $\alpha^4=\alpha^2+\alpha$
111 - $\alpha^5=\alpha^2+\alpha+1$
101 - $\alpha^6=\alpha^2+1$
001 - $\alpha^7=1$

(1) poiché $x^{2^3-1}\equiv 1 \pmod{x^3+x+1}$

x^3+x+1 è polinomio primitivo, infatti

$$x^7\equiv 1 \pmod{p(x)}$$

e 2^3-1 è ordine di x (esponente minimo per cui $x^7\equiv 1$)

(2) sono α, α^2 e α^4

$$x^3+x+1=(x-\alpha)(x-\alpha^2)(x-\alpha^4)$$

ove $p(\alpha)=0$ infatti $\alpha^3+\alpha+1=0$

$p(\alpha^2)=0$ infatti $\alpha^6+\alpha^2+1=0$

$p(\alpha^4)=0$ infatti $\alpha^{12}+\alpha^4+1=\alpha^5+\alpha^4+1=0$

(3) le radici inverse di α, α^2 e α^4 sono: α^6, α^5 e α^3

$\alpha\to\alpha^6$ infatti $\alpha\cdot\alpha^6\equiv\alpha^7\equiv 1 \pmod{p(x)}$

$\alpha^2\to\alpha^5$ $\quad\alpha^2\alpha^5\equiv 1$

$\alpha^4\to\alpha^3$ $\quad\alpha^4\alpha^3\equiv 1$

(4) I residui quadratici sono $\frac{2^3}{2}=4$ e cioè

$\alpha^2, \alpha^4, \alpha^6, 1$.

$$H=\begin{pmatrix}100 & 001\\ 011 & 001\end{pmatrix}=\begin{pmatrix}\alpha^2 & 1\\ \alpha+1 & 1\end{pmatrix}=\begin{pmatrix}\alpha^2 & 1\\ \alpha^3 & 1\end{pmatrix}$$

$$P=(101,010)(100,111)=(\alpha^2+1,\alpha)(\alpha^2,\alpha^2+\alpha+1)=(\alpha^6,\alpha),(\alpha^2,\alpha^5)$$

(5) $\det H = \alpha^2+\alpha+1=\alpha^5 \neq 0$

$\text{mcd}(\det H,\ p(x))=1$

$p(x)$ è irriducibile

$\alpha^{x \bmod 7} \equiv \alpha^x$

$\alpha^{-x} \equiv \alpha^{7-x}$

(6) $(\det H)^{-1}=\dfrac{1}{\alpha^5}=(\alpha^5)^{-1}=\alpha^2$

Allora $H^{-1}=\alpha^2\begin{pmatrix}1 & -1\\ -(\alpha+1) & \alpha^2\end{pmatrix}=\alpha^2\begin{pmatrix}1 & 1\\ \alpha+1 & \alpha^2\end{pmatrix}=$

$$H^{-1}=\begin{pmatrix}\alpha^2 & \alpha^2\\ \alpha^5 & \alpha^4\end{pmatrix}=\begin{pmatrix}\alpha^2 & \alpha^2\\ \alpha^2+\alpha+1 & \alpha^2+\alpha\end{pmatrix}$$

verifica

$$H\cdot H^{-1}=\begin{pmatrix}\alpha^2 & 1\\ \alpha^3 & 1\end{pmatrix}\begin{pmatrix}\alpha^2 & \alpha^2\\ \alpha^5 & \alpha^4\end{pmatrix}=$$

$$=\begin{pmatrix}\alpha^4+\alpha^5 & \alpha^4+\alpha^4\\ \alpha^5+\alpha^5 & \alpha^5+\alpha^4\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=I$$

ok

(7) $(C_1, C_2) = (P_1\ P_2)H =$

$$= (\alpha^6, \alpha)\begin{pmatrix} \alpha^2 & 1 \\ \alpha^3 & 1 \end{pmatrix} = (\alpha^8 + \alpha^4), (\alpha^6 + \alpha) =$$

$$= (\alpha^2, \alpha^5) = (\alpha^2, \alpha^2 + \alpha + 1)$$

$C_1 = \alpha^2 = 100$

$C_2 = \alpha^2 + \alpha + 1 = 111$

$(C_3, C_4) = (P_3, P_4)H =$

$$= (\alpha^2, \alpha^5)\begin{pmatrix} \alpha^2 & 1 \\ \alpha^3 & 1 \end{pmatrix} = (\alpha^4 + \alpha^8), (\alpha^2 + \alpha^5) =$$

$$= (\alpha^2, \alpha^3) = (\alpha^2, \alpha + 1)$$

$C_3 = \alpha^2 = 100$

$C_4 = \alpha + 1 = 011$

(8)

$(P_3, P_4) = (C_3, C_4)H^{-1} =$

$$= (\alpha^2, \alpha^3)\begin{pmatrix} \alpha^2 & \alpha^2 \\ \alpha^5 & \alpha^4 \end{pmatrix} = (\alpha^4 + \alpha^8), (\alpha^4 + \alpha^7) =$$

$$= (\alpha^2, \alpha^5) = (\alpha^2, \alpha^2 + \alpha + 1)$$

$P_3 = \alpha^4$

$P_4 = \alpha 5$

OK

$(P_1 P_2) = (C_1, C_2)H^{-1} =$

$$= (\alpha^2, \alpha^5)\begin{pmatrix} \alpha^2 & \alpha^2 \\ \alpha 5 & \alpha^4 \end{pmatrix} = (\alpha^4 + \alpha^{10}), (\alpha^4 + \alpha^9) =$$

$$= (\alpha^4 + \alpha^3), (\alpha^4 + \alpha^2) = (\alpha_6, \alpha)$$

$P_1 = \alpha^6$, $P_2 = \alpha$ OK

(g) $\begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} H = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$

deve essere $\det \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} \neq 0$ $\quad \det \underline{P} \neq 0$

$$\det \begin{pmatrix} \alpha^6 & \alpha \\ \alpha^2 & \alpha^5 \end{pmatrix} = \alpha^6 \alpha^5 - \alpha^3 = \alpha^{11} + \alpha^3 =$$
$$= \alpha^4 + \alpha^3 = \alpha^6 = \alpha^2 + 1 \neq 0$$

Allora

$$H = \begin{pmatrix} \alpha^6 & \alpha \\ \alpha^2 & \alpha^5 \end{pmatrix}^{-1} \begin{pmatrix} \alpha^2 & \alpha^5 \\ \alpha^2 & \alpha^3 \end{pmatrix} =$$

ma

$$= \begin{pmatrix} \alpha^6 & \alpha \\ \alpha^2 & \alpha^5 \end{pmatrix}^{-1} = (\det \underline{P})^{-1} \begin{pmatrix} \alpha^5 & -\alpha^2 \\ -\alpha & \alpha^6 \end{pmatrix}^T =$$
$$= \alpha \cdot \begin{pmatrix} \alpha^5 & -\alpha \\ -\alpha^2 & \alpha^6 \end{pmatrix} = \begin{pmatrix} \alpha^6 & \alpha^2 \\ \alpha^3 & 1 \end{pmatrix}$$

allora

$$H = \begin{pmatrix} \alpha^6 & \alpha^2 \\ \alpha^3 & 1 \end{pmatrix} \begin{pmatrix} \alpha^2 & \alpha^5 \\ \alpha^2 & \alpha^3 \end{pmatrix} = \begin{pmatrix} \alpha^8 + \alpha^4 & \alpha^{11} + \alpha^5 \\ \alpha^5 + \alpha^2 & \alpha^8 + \alpha^3 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^2 & 1 \\ \alpha^3 & 1 \end{pmatrix}.$$ ok!