Mobilità e Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame – 27 febbraio 2013**

Cognome e nome: *(stampatello)*
(firma leggibile)

Matricola:

NB1: In ogni esercizio, ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo.

Domanda 1
(svolgere su questo foglio nello spazio assegnato) (6 punti)

Bob adotta il *sistema di firma elettronica RSA*. Pubblica il modulo $n = 437$ e l'esponente di cifratura $e = 17$.

a) Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA.

b) Calcolare la firma A del messaggio $P = 77$.

c) Il valore $A \equiv 2 \pmod{n}$ è la firma valida di quale messaggio P?

a) $n = 437 = 19 \cdot 23$ $\varphi(n) = 396 = 2^2 \cdot 3^2 \cdot 11$ $\varphi[\varphi(n)] = 120$

$e \perp \varphi(n)$ ok

b) $A = P^d \bmod n$ $d = e^{-1} \bmod \varphi(n) = 17^{119} \bmod 396 = 233$

Meglio usare Euclide Esteso:

$396 = 23 \cdot 17 + 5$ $x_0 = 0$ $x_1 = 1$

$17 = 3 \cdot 5 + 2$ $x_2 = -q_1 x_1 + x_0 = 373$

$5 = 2 \cdot 2 + 1$ $x_3 = -q_2 x_2 + x_1 = 70$

$2 = 2 \cdot 1 + 0$ $x_4 = -q_3 x_3 + x_2 = 233$

$A = 77^{233} \bmod 437 = 248$ (square & multiply)

c) $P = A^e \bmod n = 2^{17} \bmod 437 = 409$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame – 27 febbraio 2013**

Cognome e nome: *(stampatello)*
(firma leggibile)

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (6 punti)

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 127$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 98$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 3$ non risultasse una scelta valida, Bob userà invece $\alpha = 6$ (da verificare). Se anche questa scelta non risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 110$ e spedisce il messaggio $P = 33$. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob, per un errore di trasmissione, riceve $C' = (r', t') = (37, 102)$. Calcolare il messaggio decifrato da Bob P'.

a) p primo $1 < a \leq p-2$ $1 < K \leq p-2$ $p-1 = 126 = 2 \cdot 3^2 \cdot 7$

$3^{63} \bmod 127 = 126$
$3^{42} \bmod 127 = 107$
$3^{18} \bmod 127 = 4$
} ok $\alpha = 3$ elemento primitivo di Z_{127}^*

$\beta = \alpha^a \bmod p = 3^{98} \bmod 127 = 37$

b) $r = \alpha^k \bmod p = 3^{110} \bmod 127 = 34$

$t = \beta^k \cdot P \bmod p = 37^{110} \cdot 33 \bmod 127 = 92$

c) $P' = t' \cdot r'^{-a} \bmod p = 102 \cdot 37^{98} \bmod 127 = 91$

$r^{-a} \equiv r^{p-1-a} \pmod p$

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame – 27 febbraio 2013**

Cognome e nome: *(stampatello)*
(firma leggibile)

Matricola:

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Quali sono gli elementi α dell'insieme $\mathbb{Z}_{17}^*$?

$\{1,2,3,\dots 16\}$

b) Quanti sono gli *elementi primitivi* dell'insieme $\mathbb{Z}_{17}^*$?

$\varphi(16) = 8$

c) Trovare ed elencare in ordine crescente gli elementi primitivi di $\mathbb{Z}_{17}^*$.

$\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$2^8 \equiv 1 \pmod p$
✗ $3^8 \equiv 16$ "
$4^8 \equiv 1$ "
✗ $5^8 \equiv 16$ "
✗ $6^8 \equiv 16$ "
✗ $7^8 \equiv 16$ "
$8^8 \equiv 1$ "
$9^8 \equiv 1$ "
✗ $10^8 \equiv 16$ "
✗ $11^8 \equiv 16$ "
✗ $12^8 \equiv 16$ "
$13^8 \equiv 1 \pmod p$
✗ $14^8 \equiv 16$ "
$15^8 \equiv 1$ "
$16^8 \equiv 1$ "

$\Rightarrow \alpha = \{3,5,6,7,10,11,12,14\}$

d) Qual è l'*ordine* dell'elemento $\alpha = 11$?

$\alpha = 11$ elem. primitivo $\Rightarrow Ord(11) = 16$

e) Qual è l'*ordine* dell'elemento $\alpha = 13$?

$13^1 \equiv 13 \pmod{17} \Rightarrow Ord(13) = 4$
$13^2 \equiv 16$ "
$13^3 \equiv 4$ "
$13^4 \equiv 1$ "

Domanda 4

(svolgere su questo foglio nello spazio assegnato) (5 punti)

Calcolare il logaritmo discreto $\text{Log}_\alpha(\beta)$ soluzione dell'equazione $\alpha^x \equiv \beta \pmod p$ per $p = 23$, $\alpha = 5$, $\beta = 21$, applicando l'algoritmo *Baby Step Giant Step*. Prima di tutto, verificare se esiste certamente una soluzione.

Se $\alpha = 5$ è una radice primitiva di $\mathbb{Z}_p^* \Rightarrow$ esiste 1 soluzione

$p-1 = 22 = 2 \cdot 11$ $\quad \alpha^{\frac{p-1}{q_i}} \bmod p \neq 1$ $\quad \begin{matrix} 5^2 \bmod 23 = 2 \\ 5^{11} \bmod 23 = 22 \end{matrix} \Rightarrow$ ok

$N = \lceil \sqrt{p-1} \rceil = 5$

j	α^j	k	$\beta\alpha^{-Nk}$
0	1	0	21
1	5	1	$21 \cdot 5^{17} = 8$
2	2	2	$21 \cdot 5^{12} = 10$
3	10		
4	4		
5	20		

$\alpha^j = 5^j \bmod p$

$\beta\alpha^{-Nk} \equiv \beta\alpha^{p-1-Nk} \pmod p$

$\Downarrow$

$\alpha^j \equiv \beta\alpha^{-Nk} \pmod p$ per $j=3$, $k=2$

$\alpha^{j+Nk} \equiv \beta \pmod p \Rightarrow x = j + Nk = 13$

Verifica: $5^{13} \bmod 23 = 21$ ok

Mobilità e Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame – 27 febbraio 2013**

Cognome e nome: *(stampatello)* *(firma leggibile)*

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (14 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) L'equazione $x^2 \equiv 25 \pmod{223}$ ha soluzione? Se la risposta è sì, calcolarne le radici, altrimenti risolvere $x^2 \equiv -25 \pmod{223}$. *(2 punti)*

223 primo → l'eq. ha soluzione se $25^{\frac{223-1}{2}} \equiv 1 \pmod{223}$

$25^{111} \bmod 223 = 1$ sì

Siccome $223 \equiv 3 \pmod 4 \Rightarrow X = \pm 25^{\frac{223+1}{4}} \bmod 223 =$

$= \pm 25^{56} \bmod 223 = \pm 218 =$

$= 5, 218$

2) Ricavare la sequenza binaria pseudo-casuale generata dall'algoritmo *Blum-Blum-Shab* per $p = 7$, $q = 11$, $x = 5$ e determinarne il periodo P. *(2 punti)*

i	x_i	b_i	
0	25	1	$P = 4$
1	9	1	
2	4	0	
3	16	0	
4	25	1	
5	1	1	
1			

3) Descrivere il meccanismo di memorizzazione cifrata delle password in un file pubblico per il controllo dell'accesso a un sistema. *(3 punti)*

- Come vengono cifrate? Serve un'altra chiave per leggerle?
- E quindi, in cosa consiste un attacco del vocabolario?
- Come contrastare un attacco del vocabolario? Spiegare il meccanismo nel dettaglio.

4) Descrivere le proprietà di *diffusione* e *confusione*, che secondo Claude Shannon un buon crittosistema dovrebbe avere per ostacolarne l'analisi. *(3 punti)*

Cognome e nome: *(stampatello)*
(firma leggibile)

Matricola:

5) Descrivere sommariamente l'*algoritmo AES*. Specificare: *(4 punti)*

- lunghezza delle chiavi;
- ruolo e funzioni dei *round* (ingresso, uscita, *layer*);
- funzioni dei singoli *layer*;
- elementi degni di nota nella progettazione dell' *S-Box*.