Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame 2021-22 – 25 giugno 2022**

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

Matricola:

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

Domanda 1

(svolgere su questo foglio nello spazio assegnato) (7 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 137$, $\alpha = 13$, $\beta = \alpha^a \bmod p = 90$, tenendo segreto l'esponente a ($1 < a \leq p\text{-}2$).

Bob estrae il numero casuale segreto k (*nonce*) con MCD(k, p-1) = 1. Usando sempre questo stesso valore di k, Bob calcola le seguenti firme A_1 e A_2 per i rispettivi messaggi P_1 e P_2.

$A_1 = (r_1, s_1) = (12, 24)$ $\quad P_1 = 100$
$A_2 = (r_2, s_2) = (12, 100)$ $\quad P_2 = 104$

Oscar intercetta i due messaggi firmati. Sulla base di essi e delle informazioni pubbliche, calcolare k e a (*attacco del nonce ripetuto*).

$s \equiv k^{-1}(P - ar) \pmod{(p-1)} \rightarrow sk \equiv P - ar \pmod{(p-1)}$

$\begin{cases} 24k \equiv 100 - a12 \pmod{136} \\ 100k \equiv 104 - a12 \pmod{\quad\sim} \end{cases}$

$76k \equiv 4 \pmod{136}$ $\quad MCD(76, 136) = 4 \Rightarrow$ 4 soluzioni

$19k \equiv 1 \pmod{34}$ $\quad 19^{-1} \equiv 9 \pmod{34}$

$k_0 \equiv 9 \pmod{34}$ $\quad k_i \equiv 9, 43, 77, 111 \pmod{136}$ Dai dati pubblici

$\Rightarrow \boxed{k = 77}$

$r = \alpha^k \bmod p$

$12 \equiv 13^k \bmod 137$

$24 \cdot 77 \equiv 100 - a12 \pmod{136}$

$12a \equiv 20 \pmod{136}$ $\quad MCD(12, 136) = 4 \Rightarrow$ 4 soluzioni

$3a \equiv 5 \pmod{34}$ $\quad 3^{-1} \equiv 23 \pmod{34}$ Dai dati pubblici:

$a_0 \equiv 5 \cdot 23 \equiv 13 \pmod{34}$ $\quad \beta \equiv \alpha^a \pmod{p}$

$a_i \equiv 13, 47, 81, 115 \pmod{136}$ $\quad 90 \equiv 13^a \pmod{137}$

$\Rightarrow \boxed{a = 47}$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2021-22 – 25 giugno 2022**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (5 punti)

Bob adotta il *sistema di cifratura a chiave pubblica RSA.* Pubblica il modulo $n = 17399$ e un esponente di cifratura scelto tra $e_1 = 39$, $e_2 = 1823$, $e_3 = 1113$.

a) Fattorizzare n con il metodo di Fermat. Verificare la correttezza dei dati forniti in base alle ipotesi del metodo RSA. Scegliere il valore corretto tra i tre esponenti e_1 , e_2 , e_3.

b) Alice trasmette a Bob il messaggio cifrato $C = 3$, calcolato utilizzando il valore corretto dell'esponente e. Decifrarlo e calcolare il corrispondente messaggio in chiaro P.

a) $n = 17399 = 127 \cdot 137$

$\varphi(n) = 126 \cdot 136 = 17136 = 2^4 \cdot 3^2 \cdot 7 \cdot 17$

$\varphi[\varphi(n)] = 4608$

$MCD(39, 17136) = 3$ NO
$MCD(1113, 17136) = 21$ NO
$MCD(1823, 17136) = 1$ ok
$\Rightarrow e = 1823$ $(e \perp \varphi(n))$

b) $d \equiv e^{-1} \pmod{\varphi(n)}$

Con Euclide Esteso: $d \equiv 47 \pmod{17136}$

$P = C^d \bmod n = 3^{47} \bmod 17399 = 4030$

Domanda 3

(svolgere su questo foglio nello spazio assegnato) (7 punti)

a) Spiegare cosa significa affermare che una generica funzione $y = y(x)$ è *invertibile*, ma *unidirezionale*. Perché una funzione di *hash* $h = h(x)$ non può mai essere invertibile?

b) Definire la proprietà di *unidirezionalità* di una funzione di *hash* $h = h(x)$.
Definire la proprietà di *resistenza debole alle collisioni* di una funzione di *hash* $h = h(x)$.
Mettere in evidenza per cosa differiscono le due definizioni.

c) Si consideri una ipotetica funzione di *hash* $h = h(m) = \alpha^m \bmod p$, dove p è un primo "grande e sicuro", α è un elemento generatore di $\mathbb{Z}_p^*$, e m è un intero qualsiasi. Si dica se tale funzione $h = h(m)$ è

- invertibile? (spiegare perché SI o perché NO)

NO

- unidirezionale? (spiegare perché SI o perché NO)

SI

- (almeno) debolmente resistente alle collisioni? (spiegare perché SI o perchè NO)

NO

Domanda 4

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

Alice e Bob adottano il protocollo di *Diffie-Hellman* per l'instaurazione della loro chiave simmetrica K_{AB}. Alice pubblica $p = 107$ e $\alpha = 9$. Alice sceglie $1 \le x \le p-2$ (segreto). Bob sceglie $1 \le y \le p-2$ (segreto).

Oscar osserva i numeri scambiati da Alice e Bob:

Alice ➔ Bob: $\alpha^x \equiv 13 \pmod{p}$

Alice ➔ Bob: $\alpha^y \equiv 13 \pmod{p}$

a) Oscar deduce che, per un caso fortuito, Alice e Bob hanno scelto lo stesso valore per x e y. E' corretto? Verificare se esistono più valori di x e y ($x \neq y$, $1 \le x \le p-2$, $1 \le y \le p-2$) tali che $\alpha^x \equiv \alpha^y \equiv 13 \pmod{p}$.

Test se $\alpha = 9$ è un elem. primitivo di $\mathbb{Z}_p^*$: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$

$p-1 = 106 = 2 \cdot 53$

$9^2 \equiv 81 \pmod{107}$
$9^{53} \equiv 1 \quad (\text{---})$ $\Rightarrow$ NO $\Rightarrow \exists\, x \neq y \mid \alpha^x \equiv \alpha^y \pmod{p}$

b) Sulla base delle informazioni conosciute da Oscar, calcolare gli esponenti segreti x e y con l'algoritmo Baby Step Giant Step (tutti i valori possibili se ne esistono più di uno) e la chiave K_{AB}.

$N = \lceil \sqrt{p-1} \rceil = 11$ $\quad \alpha^{-1} \equiv 12 \pmod{107}$
$\alpha^{-N} \equiv 40 \quad (\text{---})$

j	α^j	k	$\beta \cdot \alpha^{-Nk} = 13 \cdot 40^k \pmod{107}$
0	1	0	13
1	9	1	92
2	81	2	42
3	86	3	73
4	34	4	4
5	92	5	53
6	79	6	86
7	61	7	56
8	86	8	100
9	25	9	41
10	11	10	35
11		11	

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

$\Rightarrow x_1 = 5 + 11 \cdot 1 = 16$
$x_2 = 9 + 11 \cdot 6 = 69$

(per il combinaz. di x_1, x_2)

$K_{AB} = \alpha^{x \cdot y} \bmod p \equiv 9^{16 \cdot 69} \bmod 107 = 30$

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (12 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Quali sono i valori possibili dell'ordine di un elemento $\alpha \in \mathbb{Z}_{19}^*$? *(2 punti)*

1, 2, 3, 6, 9, 18

2) L'equazione $x^2 \equiv 2 \pmod{109}$ ha soluzione? Se la risposta è sì, calcolarne le radici.
L'equazione $x^2 \equiv -2 \equiv 107 \pmod{109}$ ha soluzione? Se la risposta è sì, calcolarne le radici. *(2 punti)*

$p = 109$ primo $\Rightarrow$ l'eq. ha soluzione se $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$(\pm 2)^{54} \equiv -1 \pmod{109} \Rightarrow$ nessuna delle due eq. ha soluz.,

(NB: $109 \equiv 1 \pmod{4}$)

3) Ricevi una mail da <stefano.bregni@polimi.it>, in cui il mittente presenta un certificato per "SUBJECT: Stefano Bregni" emesso da Verisign. Che procedura segui per verificare l'autenticità del certificato? Se il certificato risulta valido, puoi concludere che il mittente è il tuo Professore, oppure devi fare qualcos'altro per esserne certo? *(2 punti)*

Sicurezza delle Reti
Prof. Stefano Bregni **I Appello d'Esame 2021-22 – 25 giugno 2022**

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

Matricola:

4) Utilizzo uno *scrambler autosincronizzante* di ordine $M = 48$ per mascherare i miei dati trasmessi su un canale pubblico. Come calcolo il numero di polinomi esistenti non riducibili di grado 48, tra cui scegliere quello del mio scrambler (non è richiesto fornire i dettagli)? Scelgo un polinomio tra di essi e lo rendo pubblico. Chiunque in ascolto sul canale può leggere i miei dati? *(2 punti)*

5) Dati un algoritmo di cifratura $E_K(X)$ e rispettivo algoritmo di decifratura $D_K(X)$, si considerino le funzioni di cifratura doppia $C = E_{K_2}(E_{K_1}(P))$ e sua decifratura $P = D_{K_1}(D_{K_2}(C))$, con due chiavi K_1 e K_2 ciascuna di lunghezza $n = 32$ bit. I messaggi in chiaro P e cifrato C abbiano entrambi lunghezza 64 bit. Il calcolo delle funzioni $X = D_K(Y)$ e $Y = E_K(X)$ richiede lo stesso tempo $T = 1\,\mu s$. *(4 punti)*
Si tenta un attacco *Meet-in-the-Middle* per trovare la coppia di chiavi K_1, K_2.

a) Descrivere il procedimento. Precisare quali informazioni è necessario conoscere.
b) Quanto tempo richiede il completamento dell'attacco con successo?
c) Quale occupazione di memoria [byte] è necessaria per completare l'attacco con successo?

Servono da 2^{32} a 2^{33} operazioni $E_k(x)$ o $D_k(y)$

→ T_{tot} da 4295 a 8590 secondi (1,19 ore ÷ 2,39 ore)

$\cdot 2^{35}$ byte = 32 Gbyte