Sicurezza delle Reti

Prof. Stefano Bregni **V Appello d'Esame 2020-21 – 9 febbraio 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 cifratura a chiave pubblica di El Gamal* e pubblica $p = 127$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 33$.

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 un valore valido scelto nell'insieme $\alpha = \{4, 5\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 34$ e spedisce il messaggio $P = 50$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (92, 81)$. Calcolare il messaggio decifrato da Bob P'.

d) Calcolare il valore di k per cui Alice ha calcolato $C' = E[P']$.

a) p primo $\quad 1 < a \leq p-2 \quad p-1 = 126 = 2 \cdot 3^2 \cdot 7 \quad$ Test se α elem. prim. di $\mathbb{Z}_p^*$

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

$\left.\begin{array}{l} 3^{63} \equiv 126 \\ 3^{42} \equiv 14 \\ 3^{18} \equiv 4 \end{array}\right\} \Rightarrow \alpha = 3$ OK $\quad (\alpha = 4, 5$ no$)$ $\quad \beta = \alpha^a \bmod p = 3^{33} \bmod 127 = 10$

b) $r = \alpha^k \bmod p = 3^{34} \bmod 127 = 30$

$t = \beta^k P \bmod p = 10^{34} \cdot 50 \bmod 127 = 32 \quad \Rightarrow C = (30, 32)$

c) $P' = t' \cdot r'^{-a} \bmod p = 81 \cdot 92^{-33} \bmod 127 = 56$

$92^{-1} \equiv 29 \pmod{127}$

d) $3^k \bmod 127 = 92 \rightarrow k = 13 \quad$ (BSGS)

Sicurezza delle Reti

Prof. Stefano Bregni — **V Appello d'Esame 2020-21 – 9 febbraio 2022**

Cognome e nome: *(stampatello)*

(firma leggibile)

Matricola:

Domanda 2

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

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 103$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 24$.

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 un valore valido scelto nell'insieme $\alpha = \{4, 5\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 23$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 31$.

c) Verificare se anche la firma $A' = (r', s') = (20, 11)$ è valida da Bob per lo stesso messaggio ~~$P = 31$~~ $P=31$ e d)? Se è valida, calcolare il valore di k per cui è stata calcolata da Bob, scegliendo il metodo più veloce a disposizione.

a) p primo $\quad 1 < a < p-2 \quad k \perp p-1 \quad p-1 = 102 = 2 \cdot 3 \cdot 17$

Th.: α elem. prim. di $\mathbb{Z}_p^*$: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$$\left.\begin{aligned} 5^{51} &\equiv 102 \\ 5^{34} &\equiv 56 \\ 5^{6} &\equiv 72 \end{aligned}\right\} \Rightarrow \alpha = 5 \text{ ok } (\alpha = 3, 4 \text{ NO})$$

$\beta = \alpha^a \bmod p = 5^{24} \bmod 103 = 23$

b) $r = \alpha^k \bmod p = 5^{23} \bmod 103 = 87$

$s = k^{-1}(P - ar) \bmod (p-1) = 71(31 - 24 \cdot 87) \bmod 102 = 17$

$k^{-1} \equiv 23^{-1} \equiv 71 \pmod{102}$ $\Rightarrow A = (87, 17)$

c) $\beta^r \cdot r^s \equiv \alpha^P \pmod p$

$23^{20} \cdot 20^{11} \equiv 40 \pmod{103}$

$5^{31} \equiv 40$ $\quad (\text{———})$ $\Rightarrow A' = (20, 11)$ firma valida di $P = 31$

Invece di $5^K \equiv 20 \pmod{103}$ meglio:

$sK \equiv P - ar \pmod{(p-1)}$

$11K \equiv 31 - 24 \cdot 20 \pmod{102}$

$11K \equiv 61 \pmod{102}$ MCD$(11,102)=1 \Rightarrow$ 1 soluzione

$K \equiv 61 \cdot 65 \pmod{102}$ $11^{-1} \equiv 65 \pmod{102}$ E.E.

$\equiv 89$

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

Matricola:

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (4 punti)

a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo *Blum-Blum-Shab* per $p = 43$, $q = 47$, $x = 42$ e determinarne il periodo P. Il seme iniziale x rispetta le ipotesi del metodo?

i	x_i	b_i
0	1764	0
1	1377	1
2	431	1
3	1850	0
4	947	1
5	1506	0
6	474	0
7	345	1
8	1807	1
9	1734	0
10	1076	0
11	1764	0

$P = 11$

$n = p \cdot q = 43 \cdot 47 = 2021$

$x_0 \equiv x^2 \pmod n$

$x_i \equiv x_{i-1}^2 \pmod n$

$43 \equiv 3 \bmod 4$

$47 \equiv 3 \bmod 4$

$42 \perp 2021$

b) In base alla teoria, quali sono i valori possibili che può assumere il periodo $P = \pi(x_0)$ del generatore precedente, per valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$?

Si ricorda che $\pi(x_0)$ divide $\lambda(\lambda(n))$, dove $\lambda(n)$ è la Funzione di Charmichael, calcolabile come

$$\lambda(n) = \text{mcm}\left(\left\{\lambda\left(p_i^{a_i}\right)\right\}\right) \qquad \lambda\left(p^k\right) = \begin{cases} \frac{1}{2}\varphi\left(p^k\right) & \text{se } p = 2, k \geq 3 \\ \varphi\left(p^k\right) & \text{altrimenti} \end{cases}$$

$\lambda(n) = \text{mcm}(42, 46) = 2 \cdot 3 \cdot 7 \cdot 23 = 966$

$\lambda[\lambda(n)] = \lambda(966) = \text{mcm}(1, 2, 6, 22) = 66$

$\pi(x_0) \in \{1, 2, 3, 6, 11, 22, 33, 66\}$

Domanda 4
(svolgere su questo foglio nello spazio assegnato) (8 punti)

a) Definire la proprietà di *unidirezionalità* di una funzione di *hash* $h = h(x)$, precisando per cosa si distingue rispetto alla definizione della proprietà di *unidirezionalità* per una generica funzione invertibile $y = y(x)$.

b) Vi viene proposta una funzione di hash $h = h(m)$ che restituisce valori h di 64 bit, asserendo che è fortemente resistente alle collisioni. Desiderate provare che non è vero e vi apprestate a scrivere un programma che trovi collisioni. Che metodo pensate di seguire?

c) Sia data una funzione di hash $h = h(m)$ che restituisce stringhe pseudocasuali di lunghezza fissa 11 bit. Un attaccante tenta di ottenere un valore di hash desiderato h_0 calcolando la $h(m)$ su variazioni casuali di un messaggio malevolo m. Quanti tentativi sono necessari perché l'attacco abbia successo con probabilità almeno 0.5?

$(1-2^{-11})^n = 1/2 \rightarrow n \cong 1420$

P(successo in n prove) $= 1 - \left(1 - \frac{1}{2^{11}}\right)^n$

d) Si consideri una ipotetica funzione di *hash* $h(m) = \text{DES}_{K(m)}(\text{"111..."})$, consistente nella cifratura DES di un blocco di 64 bit "1" con chiave K pari ai primi 56 bit del messaggio m. Si dica se tale funzione $h(m)$ è

- invertibile? (spiegare perché SI o perché NO)

NO

- unidirezionale? (spiegare perché SI o perché NO)

SI

- fortemente resistente alle collisioni? (spiegare perché SI o perché NO; se si risponde NO fornire un esempio di collisione)

NO

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (10 punti)

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

1) Ricevi una mail da <stefano.bregni@polimi.it>, dove un sedicente Stefano Bregni ti contatta presentando il certificato per "SUBJECT: Stefano Bregni" emesso da Verisign. *(3 punti)*

- Che procedura segui per sincerarti dell'autenticità del certificato?
- Se la validazione del certificato va a buon fine e il certificato è quindi autentico, qual è l'informazione più importante che hai acquisito dallo stesso?
- Devi fare altro per sincerarti che il mittente sia proprio il tuo Professore? Oppure basta il certificato?

2) A invia un messaggio a B utilizzando PGP. Con che chiave A cifra il messaggio? Con che chiave A firma il messaggio? Quale chiave o quali chiavi devono essere trasmesse da A a B? Come li trasmette? *(2 punti)*

3) Utilizzo uno *scrambler autosincronizzante* di ordine M=31 per mascherare i miei dati trasmessi su un canale pubblico. Come calcolo il numero di polinomi esistenti non riducibili di grado 31, tra cui scegliere quello del mio scrambler? Scelgo un polinomio e lo rendo pubblico. Chiunque in ascolto sul canale può leggere i miei dati?*(2 punti)*

4) Illustrare il protocollo di Diffie-Helman. Dire a cosa serve e definirne le variabili. Spiegare in cosa consiste l'attacco MiM al protocollo di Diffie-Helman e illustrarne le fasi. *(3 punti)*