Sicurezza delle Reti

Prof. Stefano Bregni — **III Appello d'Esame 2021-22 – 9 settembre 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 $p = 109$, $\alpha = 9$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 64$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 9$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{2, 10\}$. 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*) $k = 5$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 100$.

c) Verificare se anche la firma $A' = (r', s') = (6, 28)$ è valida da Bob per lo stesso messaggio $P = 100$.

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 $1 < a < p-2$ $k \perp p-1$ $p-1 = 108 = 2^2 \cdot 3^3$

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

$10^{54} \equiv -1$
$10^{36} \equiv 63$ $\Rightarrow \alpha = 10$ OK ($\alpha = 2, 9$ NO)

$\beta = \alpha^a \bmod p = 10^{64} \bmod 109 = 80$

b) $r = \alpha^k \bmod p = 10^5 \bmod 109 = 47$

$s = k^{-1}(P - ar) \bmod (p-1) = 65\,(100 - 64 \cdot 47) \bmod 108 = 88$

$k^{-1} \equiv 5^{-1} \equiv 65 \pmod{108}$ $\Rightarrow$ **$A = (47, 88)$**

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

$80^6 \cdot 6^{28} \equiv 26 \pmod{109}$ $\Rightarrow A' = (6, 28)$ firma valida di $P = 100$

$10^{100} \equiv 26$ (✓)

d) Invece di risolvere $10^K \equiv 6 \pmod{109}$, meglio:

$5K \equiv P - Q \pmod{(p-1)}$

$28K \equiv 100 - 64 \cdot 6 \pmod{108}$

$28K \equiv 40 \pmod{108}$ $\quad MCD(28, 108) = 4$

$7K \equiv 10 \pmod{27}$ $\quad 7^{-1} \equiv 4 \pmod{27}$ $\Rightarrow$ 4 soluzioni

$K_0 \equiv 10 \cdot 4 \equiv 13 \pmod{27}$

$K_i \equiv 13, 40, 67, 94 \pmod{108}$

$\Rightarrow$ $K \equiv 13$

Dai dati pubblici:

$\alpha^K \equiv r \pmod{p}$

$10^K \equiv 6 \pmod{109}$

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2021-22 – 9 settembre 2022**

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

Matricola:

Domanda 2
(svolgere su questo foglio nello spazio assegnato) (7 punti)

Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 199$, $\alpha = 3$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 32$.

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 $\alpha = \{3, 4\}$. 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*) $k = 29$ e spedisce il messaggio $P = 50$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (34, 8)$. Calcolare il messaggio decifrato da Bob P'.

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

a) p primo $1 < a \leq p-2$ $p-1 = 198 = 2 \cdot 3^2 \cdot 11$ Testare α elem. primi $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\mathbb{Z}_p^*$:

$3^{99} \equiv -1$
$3^{66} \equiv 106$
$3^{18} \equiv 125$
} $\alpha = 3$ ($\alpha = 4$ NO) ok

$\beta = \alpha^a \bmod p = 3^{32} \bmod 199 = 102$

b) $r = \alpha^k \bmod p = 3^{29} \bmod 199 = 48$

$t = \beta^k P \bmod p = 102^{29} \cdot 50 \bmod 199 = 72$ $\Rightarrow$ $C = (48, 72)$

c) $P' = t' \cdot r'^{-a} \bmod p = 8 \cdot 34^{-32} \bmod 199 = 23$

d) $3^k \bmod 199 = 34$ $\rightarrow$ $k = 31$ (BSGS)

Sicurezza delle Reti
Prof. Stefano Bregni **III Appello d'Esame 2021-22 – 9 settembre 2022**

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

Matricola:

Domanda 3
(svolgere su questo foglio nello spazio assegnato) (7 punti)

a) Avete scelto una funzione di *hash* che restituisce valori di lunghezza $L = 16$ bit. In una tabella, avete memorizzato i valori di *hash* calcolati su un milione di file diversi. Qual è la probabilità che almeno due di questi file abbiano lo stesso hash in tabella?

$N = 2^{16} = 65536$
$r = 10^6$
$P \cong 1 - e^{-r^2/2N} = 1$

b) Spiegare cosa significa affermare che una *generica funzione* $y = y(x)$ è *invertibile*, ma *unidirezionale*.
Spiegare cosa significa affermare che una *funzione di hash* $y = y(x)$ (*non invertibile!)* è *non unidirezionale*.

c) Sappiamo che una certa *funzione di hash* $h = h(x)$ *non è unidirezionale*.
Dato un valore di hash h, potrebbe quindi essere possibile ricavare il messaggio m da cui è stato calcolato? Perché?

d) Si consideri una ipotetica funzione di *hash* $h = h(m) = m^7 \bmod p$, dove p è un primo tale per cui il problema del logaritmo discreto sia intrattabile in $\mathbb{Z}_p^*$ e m è un intero qualsiasi. Si spieghi perché tale funzione di hash $h = h(m)$ è unidirezionale, ma non debolmente resistente alle collisioni.

Domanda 4

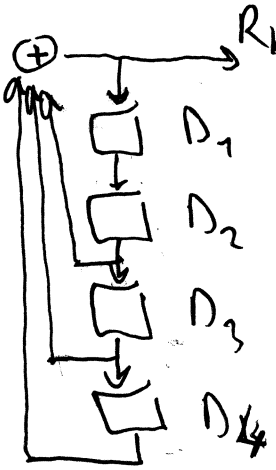
(svolgere su questo foglio nello spazio assegnato) (4 punti)

a) Si disegni lo schema di un generatore di sequenza PRBS basato su registro a scorrimento LFSR, realizzato come *scrambler autosincronizzante* con polinomio caratteristico $P(x) = x^4+x^3+x^2+1$ alimentato con tutti "0". Si indichino la sequenza binaria in ingresso con $\{I_k\} \equiv \{0\}$ e la sequenza binaria in uscita con $\{R_k\}$.

b) Si inizializzino gli elementi di ritardo D_i (i = 1, 2, 3, 4) con {0, 1, 1, 1} al passo iniziale k = 0. Ricavare la sequenza PRBS $\{R_k\}$ generata all'uscita, evidenziando la sua periodicità. Qual è il periodo P della sequenza?

c) Verificare se il polinomio $P(x)$ è irriducibile. Perché è importante fare questa verifica?

a)



b)

k	I_k	D_{1k}	D_{2k}	D_{3k}	D_{4k}	R_k
0	0	0	1	1	1	1
1	0	1	0	1	1	0
2	0	0	1	0	1	0
3	0	0	0	1	0	1
4	0	1	0	0	1	1
5	0	1	1	0	0	1
6	0	1	1	1	0	0
7	0	0	1	1	1	1

$P=7$

c) $P(x) = x^4+x^3+x^2+1$

Divisibile per x? no

" per $(x+1)$? sì

$$\Rightarrow P(x) = (x+1)(x^3+x+1)$$

$x^4+x^3+x^2+x+1 \;|\; x+1$

x^4+x^3 $\quad x^3+x^2+1$

x^2+x

x^2+x

$x+1$

$x+1$

0

Sicurezza delle Reti
Prof. Stefano Bregni — **III Appello d'Esame 2021-22 – 9 settembre 2022**

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

Matricola:

Domanda 5
(rispondere su questo foglio negli spazi assegnati) (11 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Si consideri un generatore di password consistenti di 8 simboli casuali scelti nell'alfabeto coreano, che comprende 19 consonanti e 21 vocali. Qual è la quantità di informazione [bit] delle password, se i simboli sono scelti indipendentemente una dall'altro, e la probabilità che siano una consonante o una vocale vale rispettivamente 30% e 70%? *(2 punti)*

$H(X) = -\left(0{,}3 \log_2 \frac{0{,}3}{19} + 0{,}7 \log_2 \frac{0{,}7}{21}\right) = 5{,}23$ bit/simbolo

$H(8 \text{ simboli}) = 41{,}84$ bit

2) Si calcolino tutti i residui quadratici dell'insieme $\mathbb{Z}_{11}^*$, partendo dalle potenze del suo elemento primitivo $\alpha = 6$. Esaminando i risultati ottenuti, si dica quali sono le radici quadrate di 5 (mod 11), se esistono. *(2 punti)*

$6^0 \equiv 1 \pmod{11}$
$6^2 \equiv 3$
$6^4 \equiv 9$
$6^6 \equiv 5$
$6^8 \equiv 4$

$\alpha_q = \{1, 3, 4, 5, 9\}$

$\Rightarrow \sqrt{5} \pmod{11} \equiv \pm 6^3 \equiv \pm 7 \equiv 4, 7$

3) Cos'è l'*ordine* di un elemento $\alpha \in \mathbb{Z}_p^*$? Cos'è un *elemento primitivo* dell'insieme $\mathbb{Z}_p^*$? *(2 punti)*

4) Ricevi un certificato che tra le altre include le seguenti informazioni:
Issuer name: VERISIGN;
Period of validity: from 1/1/1900 to 31/12/2199;
Subject name: MOZILLA;
Public Key of the Subject: XX;
Signature: YY.
Che procedura segui per verificare l'autenticità del certificato? *(2 punti)*

5) Con un browser web mi collego in modo sicuro a un sito alla URL https://www.esempio.edu. Dove prendo le chiavi per cifrare la mia comunicazione con il server? L'Amministratore della mia rete è a conoscenza o no del fatto che ho visitato il sito? Se il sito mi chiede una password di accesso, questa sarà leggibile dall'Amministratore della mia rete? *(3 punti)*