Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame 2018-19 – 2 luglio 2019**

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) (6 punti)

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 137$, $\alpha = 4$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 129$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 4$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{5, 7\}$. 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*) $k = 29$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 101$.

c) Verificare se anche la firma $A' = (r', s') = (117, 32)$ è valida per lo stesso messaggio $P = 101$. Se è valida, calcolare il valore di k per cui è stata calcolata da Bob.

a) p primo $1 < a < p-2$ $k \perp p-1$ α elem. prim. di Z_p^*

test: $\alpha^{(p-1)/q_i} \not\equiv 1 \pmod p$

$p-1 = 136 = 2^3 \cdot 17$

$\begin{cases} 4^{68} \equiv 1 \pmod{137} \\ 4^8 \equiv 50 \end{cases} \Rightarrow \alpha = 4$ NO

$\begin{cases} 5^{68} \equiv 136 \\ 5^8 \equiv 38 \end{cases} \Rightarrow \boxed{\alpha = 5 \text{ OK}}$

$\beta = \alpha^a \bmod p = 5^{129} \bmod 137 = (47)$

b) $r = \alpha^K \bmod p = 5^{29} \bmod 137 = (46)$

$s = K^{-1}(P - ar) \bmod (p-1) = 61\,(101 - 129 \cdot 46) \bmod 136 = (99)$

$K^{-1} \bmod (p-1) = 29^{-1} \bmod 136 = 61 \quad \Rightarrow \boxed{A = (46, 99)}$

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

$47^{117} \cdot 117^{32} \equiv 20$
$5^{101} \equiv 20$
$\Rightarrow$ $A' = (117, 32)$ firma valida di $P = 101$

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

$32K \equiv 101 - 129 \cdot 117 \pmod{136}$

$32K \equiv 104 \pmod{136}$ $\quad MCD(32, 136) = 8 \Rightarrow 8$ soluzioni

$4K_0 \equiv 13 \pmod{17}$ $\quad 4^{-1} \equiv 13 \pmod{17}$

$K_0 \equiv 16 \pmod{17}$

$K_i \equiv 16, 33, 50, 67, 84, 101, 118 \pmod{136}$

Dai dati pubblici: $r = \alpha^K \bmod p \quad 117 \equiv 5^K \pmod{137}$

$\Rightarrow \boxed{K = 33}$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2018-19 – 2 luglio 2019**

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 di El Gamal* e pubblica $p = 193$, $\alpha = 4$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 59$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 4$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{5, 6\}$. Se anche queste scelte non risultassero valide, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 67$ e spedisce il messaggio $P_1 = 200$. Calcolare il messaggio cifrato $C_1 = (r_1, t_1)$.

c) Alice estrae un nuovo numero casuale segreto (*nonce*) k e, usando sempre questo stesso valore, spedisce i messaggi P_2, P_3, P_4. Oscar intercetta i messaggi cifrati $C_2 = (r_2, t_2) = (147, 183)$, $C_3 = (r_3, t_3) = (147, 163)$, $C_4 = (r_4, t_4) = (147, 123)$ e, per altra via, viene a sapere che $P_2 = 11$. Calcolare P_3 e P_4.

a) p primo $1 < \alpha < p-2$ $\quad p-1 = 192 = 2^6 \cdot 3$

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

$\begin{cases} 4^{96} \equiv 1 \pmod{193} \\ 4^{64} \equiv 16 \end{cases} \Rightarrow \alpha = 4$ no $\quad \begin{cases} 5^{96} \equiv 192 \\ 5^{64} \equiv 84 \end{cases} \Rightarrow \alpha = 5$ ok

$\beta = \alpha^a \bmod p = 5^{29} \bmod 193 = 44$

b) $r_1 = \alpha^k \bmod p = 5^{67} \bmod 193 = 78$

$t_1 = \beta^k P \bmod p = 44^{67} \cdot 200 \bmod 193 = 22$ $\Rightarrow C_1 = (78, 22)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\quad t_2^{-1} \equiv 183^{-1} \equiv 135 \pmod{193}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \bmod p = 11 \cdot 163 \cdot 135 \bmod 193 = 33$

$P_4 = P_2 \frac{t_4}{t_2} \bmod p = 11 \cdot 123 \cdot 135 \bmod 193 = 77$

(C_2, C_3, C_4 calcolati per $K = 100$)

Sicurezza delle Reti
Prof. Stefano Bregni **I Appello d'Esame 2018-19 – 2 luglio 2019**

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

Matricola:

Domanda 3
(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 $p = 263$ e inizialmente $\alpha = 13$. Alice sceglie $1 \le x \le p-2$ (segreto). Bob sceglie $1 \le y \le p-2$ (segreto).

a) Alice verifica la correttezza dei dati secondo le ipotesi di Diffie-Hellman. Nel caso $\alpha = 13$ non risulti una scelta valida, Alice si corregge e pubblica invece $\alpha = 14$ (da verificare). Se nessuna di queste scelte risultasse valida, Alice e Bob rinunceranno a proseguire (e l'esercizio termina qui).

Test se α elem. prim. di $\mathbb{Z}_p^*$: $\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ $\quad p-1 = 262 = 2 \cdot 131$

$\begin{cases} 13^{131} \equiv 1 \\ 13^2 \equiv 169 \end{cases} \Rightarrow \alpha = 13$ No

$\begin{cases} 14^{131} \equiv 262 \\ 14^2 \equiv 196 \end{cases} \Rightarrow \boxed{\alpha = 14}$ ok

b) Oscar osserva i numeri scambiati da Alice e Bob:

Alice ➔ Bob: $\alpha^x \equiv 139 \pmod p$

Alice ← Bob: $\alpha^y \equiv 71 \pmod p$

Sulla base delle informazioni conosciute da Oscar, calcolare gli esponenti segreti x e y e la chiave K_{AB}.

$\boxed{x \equiv 55} \pmod{263}$ Tramite BSGS
$\boxed{y \equiv 39}$ (——)

$K_{AB} = \alpha^{xy} \bmod p \equiv 14^{55 \cdot 39} \equiv \boxed{175} \pmod{263}$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2018-19 – 2 luglio 2019**

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

Matricola:

Domanda 4

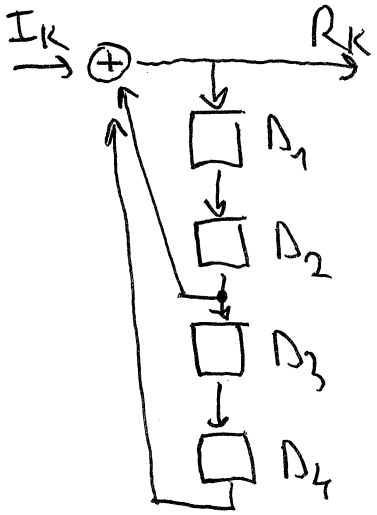
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di un generatore di sequenza PRBS basato su registro a scorrimento LFSR, realizzato come *scrambler autosincronizzante* con polinomio caratteristico $P(x) = 1+x^2+x^4$ 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 $\{0, 1, 0, 0\}$ 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. Se lo fosse, quali sarebbero i valori possibili di P?

a)



b)

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

$P=6$

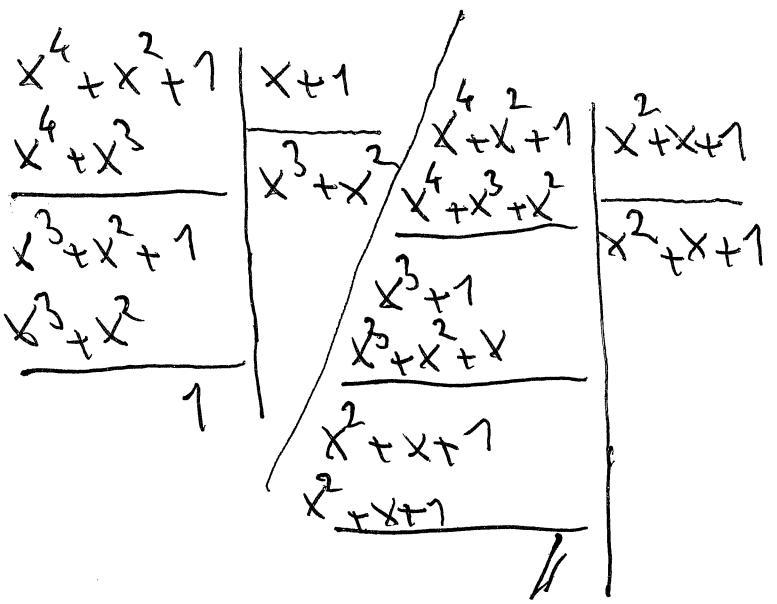
c) $P(x) = x^4+x^2+1$

Divisibile per x? NO

Divisibile per $x+1$? NO

Divisibile per x^2+x+1? SI

$\Rightarrow P(x) = (x^2+x+1)^2$



Se $P(x)$ riducibile:

$P \setminus 15 \quad P \in \{1, 3, 5, 15\}$

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

Matricola:

Domanda 5

(rispondere su questo foglio negli spazi assegnati) (15 punti)
(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

1) Si consideri un generatore di password composte da 20 caratteri casuali X scelti nell'alfabeto inglese di 26 caratteri. *(3 punti)*
a) Qual è la quantità di informazione [bit] delle password, se i 26 caratteri sono equiprobabili?
b) Qual è la quantità di informazione delle password, se invece la probabilità che X sia una vocale è 0.50, e le consonanti sono equiprobabili?

a) $P(X=x_i) = \frac{1}{26}$ $H(X) = -\sum_{1}^{26} \frac{1}{26} \log_2 \frac{1}{26} = 4{,}7$ bit/carattere

$\Rightarrow H(20 \text{ caratteri}) = 94$ bit

b) $P(X=\text{vocale}) = 0{,}50/5$

$P(X=\text{consonante}) = 0{,}50/21$

$H(X) = -\left[0{,}50 \log_2 0{,}10 + 0{,}50 \log_2 \frac{0{,}50}{21}\right] = 4{,}357$ bit/carattere

$\Rightarrow H(20 \text{ caratteri}) = 87{,}14$ bit

2) Nella suite di protocolli *Transport Level Security (TLS)*, quali sono i passi principali e le funzioni svolte dallo *Handshake Protocol*? Quante chiavi sono create e per quali scopi? *(4 punti)*

3) Definire la proprietà *"fortemente resistente alle collisioni"* per una buona funzione di hash. Si consideri la funzione $h(x) = \mathrm{LSB}_{16}(x^4)$, che restituisce i 16 bit meno significativi di x^4, con x intero. Provare che $h(x)$ non è fortemente resistente alle collisioni. *(2 punti)*

4) Si supponga di avere un sistema di autenticazione di utenti basato su biometria. Il pattern del candidato k è confrontato con il pattern memorizzato per l'utente A, misurandone la *distanza* $d_{k\mathrm{A}}$ secondo un'opportuna metrica. Il candidato è accettato come A se $d_{k\mathrm{A}} < D$. Suggerire come scegliere la soglia di accettazione D e spiegare pro e contro di una scelta non ottimale. *(2 punti)*

5) Si presenti a grandi linee l'algoritmo di creazione della chiave di round (*key schedule*) in AES. *(3 punti)*