Sicurezza delle Reti

Prof. Stefano Bregni — **IV Appello d'Esame 2024-25 – 21 gennaio 2026**

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 $p = 109$, $\alpha = 6$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 69$.

a) Si rende noto che $\alpha = 6$ è una radice primitiva di $\mathbb{Z}_{109}^*$. Calcolare β.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 101$. Per questo valore di k, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 12$.

c) Verificare se anche la firma $A' = (r', s') = (10, 42)$ è valida da Bob per il messaggio $P = 12$.

d) Se è valida, calcolare il valore di k per cui è stata calcolata da Bob risolvendo l'equazione $s \equiv 42 \pmod{p\text{-}1}$ (non *Baby Step Giant Step*).

a) p primo $1 \le a \le p-2$ $K \perp p-1$ $p-1 = 108 = 2^2 \cdot 3^3$ $\beta = \alpha^a \bmod p = 6^{69} \bmod 109$
$= 32$

b) $r = \alpha^k \bmod p = 6^{101} \bmod 109 = 50$

$s = k^{-1}(P - ar) \bmod (p-1) = 77(12 - 69 \cdot 50) \bmod 108 = 90$ $\Rightarrow A = (50, 90)$

$k^{-1} \equiv 101^{-1} \equiv 77 \pmod{108}$

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

$32^{10} \cdot 10^{42} \equiv 16 \pmod{109}$
$6^{12} \equiv 16 \pmod{109}$
$\Rightarrow$ OK $A' = (10, 42)$ firma valida di $P = 12$

d) $K_S \equiv P - a_1 \pmod{(p-1)}$

$42K \equiv 12 - 69 - 10 \pmod{108}$

$42K \equiv -30 \pmod{108}$ $\quad MCD(42, 108) = 6 \Rightarrow$ 6 soluzioni

$7K \equiv -5 \pmod{18}$

$\rightarrow K_0 \equiv 7 \pmod{18}$

$\Rightarrow K_i \equiv 7, 25, 43, 61, 79, 97 \pmod{108}$

Dai dati pubblici: $6^K \equiv 10 \pmod{109}$

$\Rightarrow K = 25$

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2024-25 – 21 gennaio 2026**

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 $p = 197$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 103$.

a) Si rende noto che $\alpha = 5$ è una radice primitiva di $\mathbb{Z}_{197}^*$. Calcolare β.

b) Alice estrae il numero casuale segreto (*nonce*) $k = 58$ e spedisce il messaggio $P = 100$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

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 $C_2 = (r_2, t_2) = (99, 40)$, $C_3 = (r_3, t_3) = (99, 108)$, $C_4 = (r_4, t_4) = (99, 60)$ e, per altra via, viene a sapere che $P_2 = 99$. Calcolare P_3 e P_4.

a) $\beta = \alpha^a \bmod p = 5^{103} \bmod 197 = 27$

b) $r_1 = \alpha^k \bmod p = 5^{58} \bmod 197 = 47$

$t_1 = \beta^k \cdot P_1 \bmod p = 27^{58} \cdot 100 \bmod 197 = 55$

$\Rightarrow C_1 = (47, 55)$

c) $\frac{t_2}{P_2} \equiv \frac{t_3}{P_3} \equiv \frac{t_4}{P_4} \equiv \beta^k \pmod p$ $\quad t_2^{-1} = 40^{-1} \equiv 133 \pmod{197}$

$P_3 \equiv P_2 \frac{t_3}{t_2} \pmod p \equiv 99 \cdot 108 \cdot 133 \equiv 90 \pmod{197}$

$P_4 \equiv P_2 \frac{t_4}{t_2} \pmod p \equiv 99 \cdot 60 \cdot 133 \equiv 50 \pmod{197}$

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2024-25 – 21 gennaio 2026**

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

Matricola:

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

Bob adotta il *sistema di cifratura a chiave pubblica RSA*. Pubblica il modulo $n = 24613$ e un esponente di cifratura scelto tra $e_1 = 513$, $e_2 = 917$, $e_3 = 921$.

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 $C = 82$, calcolato utilizzando il valore corretto dell'esponente e. Decifrarlo e calcolare il corrispondente messaggio in chiaro P.

a) $n = 24613 = 151 \cdot 163$ (p, q primi)

$\varphi(n) = 150 \cdot 162 = 24300 = 2^2 \cdot 3^5 \cdot 5^2$

$MCD(513, 24300) = 27$

$MCD(917, 24300) = 1 \Rightarrow e = 917$

$MCD(921, 24300) = 3$

$e \perp \varphi(n)$

i	$n + i^2$
1	24614
2	24617
3	24622
4	24629
5	24638
6	$24649 = 157^2$

$\Rightarrow n = (157-6)(157+6)$

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

Con Euclide Esteso: $d = 53$

$24300 = 26 \cdot 917 + 458$

$917 = 2 \cdot 458 + 1$

$x_0 = 0 \quad x_1 = 1$

$x_2 = (-26)(1) + 0 = -26$

$x_3 = (-2)(-26) + 1 = 53$

$P = C^d \bmod n = 82^{53} \bmod 24613$

$= 3050$

Domanda 4

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

a) Definire la proprietà di *unidirezionalità* di una *generica funzione invertibile* $y = y(x)$ e di una *funzione di hash* $y = h(x)$ (necessariamente non invertibile).

b) Adottate una versione semplificata di SHA a 64 bit come funzione di *hash* per la vostra Organizzazione. Conservate gli *hash* delle password (segrete) di tutti i vostri utenti. Suggerite un modo per ricavare dall'*hash* la password di un utente che vi interessa e autenticarvi al suo posto.

c) Si consideri una ipotetica funzione di hash $h = h(m) = \mathrm{AES}_{"11\ldots1"}(m_{128})$, definita come la cifratura AES degli ultimi 128 bit (i 128 bit meno significativi) del messaggio m con chiave pari a 128 cifre "1".

Si dica se tale funzione $h = h(m)$ è:

- invertibile? (spiegare perché SI o perché NO)

- unidirezionale? (spiegare perché SI o perché NO)

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

Sicurezza delle Reti
Prof. Stefano Bregni — **IV Appello d'Esame 2024-25 – 21 gennaio 2026**

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) Bob adotta il *sistema di cifratura a chiave pubblica di El Gamal* e pubblica $p = 317$, $\alpha = 27$, $\beta = \alpha^a \bmod p = 50$, tenendo segreto l'esponente $a = 301$. Decifrare il messaggio $C = (r, t) = (13, 48)$. *(2 punti)*

$P = t \cdot r^{-a} \bmod p =$

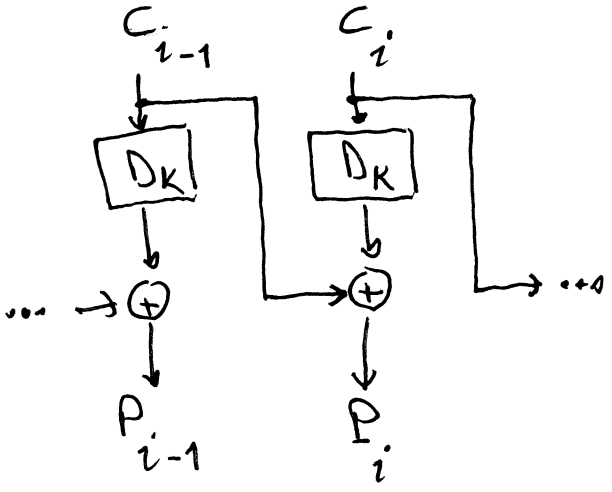
$= 48 \cdot 13^{-301} \bmod 317 = 48 \cdot 13^{15} \bmod 317 = 107$

2) Dopo l'ultima lezione, il vs. Prof. ha dimenticato un foglietto in aula con su scritto "GDHQWCI (8, 9, 1, 10)". Provate a decifrare immaginando che abbia annotato la sua password codificata attraverso il *Cifrario di Vigenère* (mod 26) con chiave $K = (8, 9, 1, 10)$. Cosa ricavate? *(2 punti)*

YUGGOTH

Alfabeto	
0	a
1	b
2	c
3	d
4	e
5	f
6	g
7	h
8	i
9	j
10	k
11	l
12	m
13	n
14	o
15	p
16	q
17	r
18	s
19	t
20	u
21	v
22	w
23	x
24	y
25	z

3) Si consideri un cifrario a blocchi concatenato secondo la modalità *Cipher Block Chaining* (CBC), in cui cifratura e decifratura sono svolte rispettivamente come $C_i = E_K(P_i \oplus C_{i-1})$ e $P_i = C_{i-1} \oplus D_K(C_i)$, C_0 è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 1024 bit. Disegnare lo schema a blocchi del processo di decifrazione. Il flusso cifrato $\{C_i\}$ subisce errori di trasmissione puramente casuali con tasso ε. Quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$ nei due casi $\varepsilon = 0.5$ e $\varepsilon = 10^7$? *(2 punti)*



$\varepsilon = 0,5 \rightarrow \varepsilon = 0,5$

$\varepsilon = 10^{-7} \rightarrow \varepsilon = 5 \cdot 10^{-5}$

4) Trovare i fattori primi di $n = 15403$ attraverso l'*Algoritmo di Fattorizzazione p−1* di Pollard con base $a = 3$. *(2 punti)*

$b_1 \equiv 3 \pmod{15403}$

$b_2 \equiv 3^2 \equiv 9 \ (n) \quad MCD(8, 15403) = 1$

$b_3 \equiv 9^3 \equiv 729 \ (n) \quad MCD(728, 15403) = 1$

$b_4 \equiv 729^4 \equiv 5257 \ (n) \quad MCD(5256, 15403) = 73$

$\Rightarrow p = 73$

$q = 211$

5) Su Astalavista, hai trovato un certificato in cui leggi, tra le altre cose: *(2 punti)*

Issuer name: TrueServices.Inc;
Period of validity: from 1/1/1990 to 31/12/2199;
Subject name: STEFANO.BREGNI@POLIMI.IT;
Public Key of the Subject: XXXXXXXXXXXXXXXXXXX
Signature: YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY.

Sostituisci i tre parametri *Subject name / Public Key of the Subject / Signature* rispettivamente con: il tuo nome, la tua P.K., la tua firma. Il certificato è formalmente valido? Se no, cosa hai sbagliato?

6) Avete un messaggio m e la sua firma A (firma RSA dell'hash SHA-2 256). Suggerite un modo per stimare il numero totale di messaggi per cui lo stesso A sia una firma valida. *(2 punti)*