Sicurezza delle Reti

Prof. Stefano Bregni — **I Appello d'Esame 2022-23 – 22 giugno 2023**

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 $p = 103$, $\alpha = 5$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 101$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 5$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{7, 8\}$. 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*) $k = 54$ e spedisce il messaggio $P = 100$ a Bob. Calcolare il messaggio cifrato $C = (r, t)$.

c) Bob riceve $C' = (r', t') = (26, 4)$. Calcolare il messaggio decifrato da Bob P'.

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

a) p primo $1 < a \leq p-2$ $p-1 = 102 = 2 \cdot 3 \cdot 17$ Tutti α elem. prim. $\mathbb{Z}_p^*$

$\alpha^{\frac{p-1}{q_i}} \equiv 1 \pmod p$

$5^{51} \equiv 102$
$5^{34} \equiv 56$
$5^{6} \equiv 72$
$\Rightarrow$ $\alpha = 5$ OK ($\alpha = 7, 8$ NO)

$\beta = \alpha^a \bmod p = 5^{101} \bmod 103 = 62$ ($\equiv 5^{-1}$)

b) $r = \alpha^k \bmod p \equiv 5^{54} \bmod 103 \equiv 81$

$t = \beta^k P \bmod p \equiv 62^{54} \cdot 100 \bmod 103 \equiv 61$ $\Rightarrow$ $C = (81, 61)$

c) $P' \equiv t' \cdot r'^{-a} \bmod p = 4 \cdot 26^{-101} \bmod 103 \equiv 4 \cdot 26 \bmod 103 = 1$

d) $5^K \bmod 103 \equiv 26$ $N = \lceil \sqrt{p-1} \rceil = 11$ $\alpha^{-1} \equiv 62 \pmod{103}$

$\alpha^{-N} \equiv 88$ ($\frown$)

j	α^j	K	$\beta \cdot \alpha^{-NK}$
0	1	0	26
1	5	1	(22)
2	25	2	
3	(22)		

$\rightarrow 26 \cdot 88^K$

$\Rightarrow$ $K = 3 + N \cdot 1 = (14)$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2022-23 – 22 giugno 2023**

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

Matricola:

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

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 163$, $\alpha = 11$, $\beta = \alpha^a \bmod p = 149$, 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.

$A_1 = (r_1, s_1) = (120, 2)$ $\quad P_1 = 32$
$A_2 = (r_2, s_2) = (120, 24)$ $\quad P_2 = 36$

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

$S \equiv K^{-1}(P - ar) \pmod{(p-1)} \rightarrow SK \equiv P - ar \pmod{(p-1)}$

$$\begin{cases} 2K \equiv 32 - a120 \pmod{162} \\ 24K \equiv 36 - a120 \pmod{162} \end{cases}$$

$22K \equiv 4 \pmod{162}$ $\quad MCD(22, 162) = 2 \Rightarrow$ 2 soluzioni

$11K \equiv 2 \pmod{81}$ $\quad 11^{-1} \equiv 59 \pmod{81}$

$\rightarrow K_0 \equiv 37 \pmod{81}$

$K_i \equiv 37, 118 \pmod{162}$

$\Rightarrow \boxed{K = 37}$

Dai dati pubblici:
$r \equiv \alpha^K \bmod p$
$11^{37} \equiv 120 \pmod{163}$

$2 \cdot 37 \equiv 32 - a120 \pmod{162}$

$a120 \equiv 120 \pmod{162}$ $\quad MCD(120, 162) = 6 \Rightarrow$ 6 soluzioni

$20a \equiv 20 \pmod{27}$

$\rightarrow a_0 \equiv 1 \pmod{27}$

$a_i \equiv 1, 28, 55, 82, 109, 136,$

$\Rightarrow \boxed{a = 55}$

Dai dati pubblici:
$\beta \equiv \alpha^a \pmod{p}$
$11^{55} \equiv 149 \pmod{163}$

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2022-23 – 22 giugno 2023**

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

Matricola:

Domanda 3

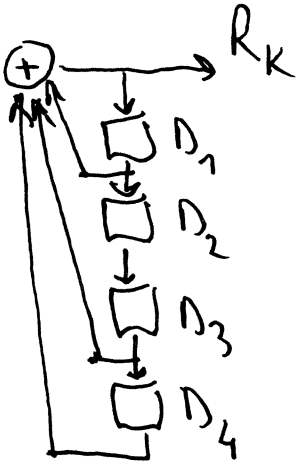
(svolgere su questo foglio nello spazio assegnato) (5 punti)

a) Si disegni lo schema di un generatore di sequenza PRBS basato su registro a scorrimento LFSR, realizzato come *scrambler autosincronizzante* con polinomio caratteristico $P(x) = x^4+x^3+x+1$ alimentato con tutti "1". Si indichino la sequenza binaria in ingresso con $\{I_k\} \equiv \{1\}$ 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, 0, 1, 1} al passo iniziale $k = 0$. Ricavare la sequenza PRBS $\{R_k\}$ generata all'uscita, evidenziando la sua periodicità. Qual è il periodo Π della sequenza?

c) Verificare se il polinomio $P(x)$ è irriducibile. Se non lo è, scomporlo in fattori (polinomi irriducibili). Il periodo Π riscontrato al passo b) è uno dei valori previsti dalla teoria nel caso in cui $P(x)$ sia irriducibile?

a)



b)

K	I_K	D_{1K}	D_{2K}	D_{3K}	D_{4K}	R_K
0	1	0	0	1	1	1
1	1	1	0	0	1	1
2	1	1	1	0	0	0
3	1	0	1	1	0	0
4	1	0	0	1	1	1
5	1	⋮	⋮	⋮	⋮	
6	1	⋮	⋮	⋮	⋮	
⋮	⋮					

$\Pi = 4$

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

Divisibile per $(x+1)^2$

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

$x^4+x^3+x+1 \;|\; x+1$
$x^4+x^3 \quad\quad x^3+1$
$x+1$
$x+1$
//

$x^3+1 \;|\; x+1$
$x^3+x^2 \quad\quad x^2+x+1$
x^2+1
x^2+x
$x+1$
$x+1$
//

$\Pi \notin \{1, 3, 5, 15\}$

$\Pi \times (2^4-1)$

Domanda 4

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

a) Abbiamo facilmente verificato che una certa *funzione di hash* $h = h(x)$ *non è unidirezionale*.
Conoscendo un certo valore di hash $\overline{h}$, possiamo quindi ricavare il messaggio $\overline{m}$ da cui è stato calcolato come $\overline{h} = h(\overline{m})$? Perché?

Sì, se la funzione di hash non è unidirezionale, allora conoscendo un valore di hash h' possiamo trovare almeno un messaggio m' tale che h(m') = h'.
Questo perché una funzione non unidirezionale è facilmente invertibile, quindi dato l'hash è possibile risalire al messaggio che lo ha generato, oppure a un messaggio qualsiasi che produce lo stesso valore di hash.

In altre parole, la funzione non offre protezione: chi conosce h' può trovare m' usando tecniche computazionali efficienti, come una tabella precalcolata o un algoritmo di inversione.

b) Avete scelto una funzione di *hash* $h = h(m)$ che restituisce valori di lunghezza $L = 56$ bit. In ciascuna di due tabelle, avete memorizzato i valori di *hash* calcolati su un miliardo di file diversi (2 miliardi di file diversi in tutto). Qual è la probabilità che almeno un valore nella prima tabella sia anche nella seconda?

$N = 2^{56} = 7.2 \cdot 10^{16}$ $P \cong 1 - e^{-r^2/N} \cong 1 - e^{-13.88} \cong 1 - 9.4 \cdot 10^{-7} \cong$

$r = 10^9$ $\cong 0,9999999$

c) Come lavoro di Tesi di Laurea, hai progettato la funzione di hash $h = supremeH(m)$ che restituisce valori nell'intervallo $0 \le h \le 10^{16}$. Calcolare $supremeH(m)$ richiede 1 ns sulla macchina più veloce in commercio. Una Fondazione mette a disposizione 1000 Euro, da offrire in premio a chi vince una delle seguenti sfide pubbliche a tua scelta:
1) provare entro 24 ore che $supremeH(m)$ non è debolmente resistente alle collisioni;
2) provare entro 24 ore che $supremeH(m)$ non è fortemente resistente alle collisioni.
Se nessuno vince la sfida, il premio va a te, in quanto ideatore di $supremeH(m)$.

- Quale sfida scegli di bandire? Perché? Per bandirla, quali informazioni devi pubblicare, oltre all'algoritmo di calcolo di $supremeH(m)$?

Questa sfida è più difficile da vincere rispetto alla sfida 1, perché per violare la forte resistenza alle collisioni bisogna trovare due messaggi qualsiasi distinti m1 e m2 tali che supremeH(m1) = supremeH(m2), senza conoscere nessun valore di hash in partenza.

Invece, la sfida 1 (contro la debole resistenza) richiede di trovare un messaggio m2 che collide con un hash h già noto (quindi più semplice). Quindi, bandisco la sfida più difficile in modo da massimizzare le mie probabilità di vincere il premio.

Devo pubblicare: l'algoritmo completo per calcolare supremeH(m), così che i partecipanti possano implementarlo e testarlo.

- Descrivere la tecnica di forza bruta per vincere la sfida 1). Quanto tempo serve?

116 giorni per vincere con probabilità 63%

Sicurezza delle Reti
Prof. Stefano Bregni — **I Appello d'Esame 2022-23 – 22 giugno 2023**

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) Si consideri un generatore di password consistenti di 12 simboli casuali scelti nell'alfabeto greco, che comprende 17 consonanti e 7 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 25% e 75%? *(2 punti)*

$H(\cdot) = -\left(0{,}25 \log_2 \frac{0{,}25}{17} + 0{,}75 \log_2 \frac{0{,}75}{7}\right) = 1{,}522 + 2{,}417 = 3{,}94$ bit/simbolo

$H(12 \text{ simboli}) = 47.26$ bit

2) Quali sono i valori che può assumere il periodo $\Pi = \pi(x_0)$ delle sequenze PRBS generate dall'Algoritmo *Blum-Blum-Shab* per $p = 31$, $q = 59$ e valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$? *(2 punti)*

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

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

$\lambda(n) = \text{mcm}(30, 58) = 2 \cdot 3 \cdot 5 \cdot 29 = 870$

$\lambda[\lambda(n)] = \lambda(870) = \text{mcm}(1, 2, 4, 28) = 28$

$\Pi(x_0) \in \{1, 2, 4, 7, 14, 28\}$

Text

3) Quanti sono i *residui quadratici* nell'insieme $\mathbb{Z}_{701}^*$? ($p = 701$ primo) *(2 punti)*

350

Z_701 è l'insieme dei numeri da 1 a 700 che sono invertibili modulo 701. Poiché 701 è primo, **Z_701 ha 700 elementi**.

In un campo Z*_p con p primo, la metà degli elementi (escludendo lo 0) sono residui quadratici, cioè numeri che sono il quadrato di qualche altro elemento del campo.

Quindi: Numero di residui quadratici in Z*_701 = 700 / 2 = 350

4) Ricevi una mail da <donaldtrump@whiteouse.gov>, in cui il mittente ti invita a un cocktail in Florida (a pagamento) e per accreditarsi presenta un certificato emesso da Verisign avente come SUBJECT l'ex presidente Donald Trump. Che procedura segui per verificare l'autenticità del certificato? Se il certificato risulta valido, puoi essere ragionevolmente certo che il mittente sia l'ex POTUS? Perché si o perché no? *(2 punti)*

1. Verifica dell'autenticità del certificato (procedura):
- Verifico che il certificato sia digitally signed da Verisign, una Certification Authority (CA) fidata.
- Controllo la firma digitale con la chiave pubblica di Verisign (che è nota e memorizzata nel sistema operativo o nel browser).
- Controllo che il certificato sia ancora valido nel tempo (non scaduto).
- Controllo che non sia stato revocato, consultando la CRL (Certificate Revocation List) o tramite OCSP.
- Controllo che il campo SUBJECT riporti effettivamente "Donald Trump".

2. Il certificato è valido. Posso essere certo che il mittente sia davvero Donald Trump?
No, non posso esserne certo, e il motivo è questo:
- Un certificato digitale attesta l'identità della chiave pubblica, non del mittente dell'email.
- Chi mi ha inviato la mail potrebbe aver ottenuto il certificato in modo fraudolento, oppure qualcun altro potrebbe aver avuto accesso alla corrispondente chiave privata.
- Inoltre, l'indirizzo email può essere falsificato (email spoofing).
- In assenza di autenticazione dell'intero messaggio con la chiave privata corrispondente al certificato, non posso sapere se è stato davvero firmato da chi dice di essere.

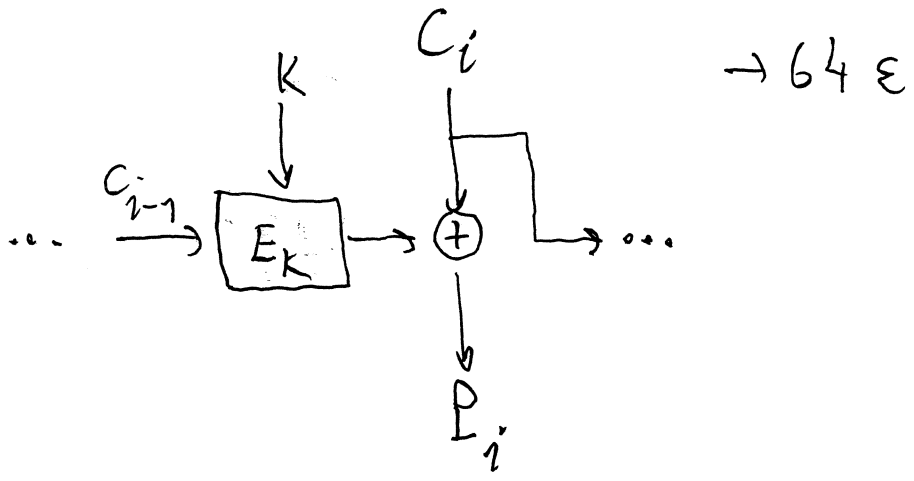
5) Si consideri un sistema di autenticazione di utenti basato su biometria. Cosa significa rilevare empiricamente che FRR = 1? *(2 punti)*

FRR (False Rejection Rate) indica la probabilità che il sistema rifiuti un utente legittimo, cioè non riconosca correttamente una persona autorizzata.

Dire che FRR = 1 significa che il sistema, nella pratica, rifiuta il 100% degli utenti legittimi: nessun utente autorizzato riesce ad autenticarsi.

Questo è un comportamento gravissimo, perché rende il sistema completamente inutilizzabile anche da chi ha accesso.

6) Si consideri un cifrario a blocchi concatenato secondo il *Cipher FeedBack Mode* (CFB), in cui cifratura e decifratura sono svolte rispettivamente come $C_i = P_i \oplus E_K(C_{i-1})$, $P_i = C_i \oplus E_K(C_{i-1})$, C_0 è il vettore di inizializzazione, la dimensione dei blocchi P_i e C_i è 128 bit. Se il flusso cifrato $\{C_i\}$ subisce errori di trasmissione puramente casuali con tasso ε molto piccolo (ossia, gli errori sono rari ed isolati), quale sarà il tasso di errore sul flusso decifrato $\{P_i\}$? Per rispondere, può essere utile disegnare lo schema a blocchi del processo di decifrazione. *(2 punti)*



→ 64 ε