Eserciziario CS

RSA

- p e q devono essere primi
- $n = pq$
- $\phi = (p-q)(q-1)$
- $1 < e < \phi$ con n e ϕ coprimi
- $ed \, mod \phi = 1$
- dimensione dei blocchi $log_2(n)$

$C = M^e mod n$

$M = C^d mod n$

Es 4 del 6 giugno 2006

$p = 7 \quad q = 3 \quad e = 5$

- Calcolare C del testo $M = 4$

$n = pq = 7 * 3 = 21$

$C = M^e mod n = 4^5 mod 21 = 16$

- Calcolare la chiave (d, n)

$\phi = (7-1)(3-1) = 12$

$ed \, mod \phi = 1 \quad \rightarrow \quad 5 * d \, mod 12 = 1 \quad \rightarrow \quad d = 5$

Diffie-Hellman

- q e α sono primi
- A e B generano randomicamente X_A e X_B minori di q

$Y_A = \alpha^{X_A} mod q \qquad Y_B = \alpha^{X_B} mod q$

$K_A = Y_B^{X_A} mod q \qquad K_B = Y_A^{X_B} mod q \qquad K_A = K_B$

Es 5 del 20 giugno 2006

$Y_A = 5 \qquad Y_B = 8 \qquad q = 11 \qquad \alpha = 2$

$5 = 2^{X_A} mod 11 \qquad \rightarrow \qquad X_A = 4$

$8 = 2^{X_B} mod 11 \qquad \rightarrow \qquad X_B = 3$

$K_A = 8^4 mod 11 = 4$

$K_B = 5^3 mod 11 = 4$

Bell-La Padula

(r_2, c_2) domina (r_1, c_1) se e solo se $r_1 \leq r_2 \land c_1 \subseteq c_2$

- No Read_Up : $R_{obj} \leq R_{sub} \land C_{obj} \subseteq C_{sub}$
- No Write_Down : $R_{sub} \leq R_{obj} \land C_{sub} \subseteq C_{obj}$

Es 7 giugno 2006

subject: (secret, {red, green, blue})

1. (top secret, {red})

$top\_secret \leq secret \land \{red\} \subseteq \{red, green, blue\}$ FALSE

$secret \leq top\_secret \land \{red, green, blue\} \subseteq \{red\}$ FALSE

NESSUN PERMESSO

2. (secret, {red})

$secret \leq secret \land \{red\} \subseteq \{red, green, blue\}$ TRUE

$secret \leq secret \land \{red, green, blue\} \subseteq \{red\}$ FALSE

SOLO LETTURA

7. (top secret, {red, green, blue, black})

$top\_secret \leq secret \land \{red, green, blue, bleck\} \subseteq \{red, green, blue\}$ FALSE

$secret \leq top_secret \land \{red, green, blue\} \subseteq \{red, green, blue, black\}$ TRUE

SOLO SCRITTURA

Affine

$E(M) = (a * M + b) mod |A|$

- a e A devono essere relativamente primi
- a e b sono interi positivi
- a chiave di cifratura
- A dimensioe dell'alfabeto

$D(C) = a^{-1} * (C - b) mod |A|$

- $(a^{-1} * a) mod |A| = 1$

Vigenère

Es 1 del 14 giugno 2007

Plaintext: * U A * * I A I * * E R I * * E

Ciphertext: I * E C F A * * O H * C K S P *

$k_1 = 2$

$k_2 = 18$

$k_3 = 4$

$k_4 = 11$

Plaintext: GUARDIAIMPERIALE

Link VS End-to-End

Link	End-to-End
il messaggio é esposto nel mittente/destinatario	il messaggio é criptato nel mittente/desinatario
il messaggio é esposto nei nodi intermedi	il messaggio é criptato nei nodi intermedi
sono applicate dall'host mittente/destinatario	sono applicate dal processo mittente/destinatario
sono trasparenti all'utente	l'utente applica la cripazione
host mantiene una struttura di criptazione	l'utnete deve determinare l'algoritmo
una struttura unica per tutti	l'utnte seleziona lo schema di criptazione software
può essere fatto dall'hardware	implementazione software
o tutti i messaggi o nessuno é criptato	l'utente seglie se criptare o meno il messaggio
c'é bisogno di una chiave per ogni host-intermediate node	richiede una chiave per coppia di utenti
fornisce l'autenticazione dell'host	fornisce l'autenticazione dell'utente