Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: B. Masucci

Appello del 15/02/2006

Non è ammesso alcun materiale per la consultazione (pena l'annullamento del compito). Avete due ore a disposizione. Buon lavoro!

1	2	3	4	totale
/25	/25	/25	/25	/100

1. (25 punti) Si consideri il seguente crittosistema: Data una stringa k di m caratteri ed un testo in chiaro in inglese di $n=t \cdot m$ caratteri, con $t>1$, si costruisce una chiave di n caratteri concatenando le t stringhe $s_1,\ldots,s_t$, di lunghezza m, dove
   - $s_1 = k$,
   - Per $i=2,\ldots,t$, la stringa s_i è ottenuta da s_{i-1} shiftando di j posti a destra (mod 26) il j-esimo carattere di s_{i-1}, con $j=1,\ldots,m$.
   - Ad esempio, considerando l'usuale corrispondenza tra l'alfabeto inglese e i numeri da 0 a 25:

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

   se k= CRYPT e n=15, la chiave ottenuta è: CRYPTDTBTYEVEXD.

   Il testo cifrato si ottiene effettuando la somma modulo 26 del testo in chiaro e della chiave costruita come sopra.
   Si analizzi la sicurezza del crittosistema rispetto ad un ciphertext-only attack, spiegando in dettaglio i passi da effettuare per risalire al testo in chiaro.

2. (25 punti) Funzioni hash.
   Si consideri la funzione hash H definita come segue: Dato un messaggio $M= X_1X_2 \ldots X_n$ costituito da n blocchi di 64 bit e dato un valore iniziale H_0 di 64 bit, sia $H(M)=H_n$, dove $H_i = DES_{g(H_{i-1})}[X_i] \oplus X_i$, con $i=1,\ldots,n$ e $g:\{0,1\}^{64} \rightarrow \{0,1\}^{56}$.
   Si utilizzi la proprietà del complemento di DES per mostrare che H non soddisfa la proprietà di sicurezza debole.
   - Suggerimento: si utilizzi il fatto che per ogni coppia di stringhe binarie A ed E si ha $\bar{A} \oplus \bar{E} = A \oplus E$.

3. (25 punti) Crittosistema RSA.
    - (5 punti) Si descrivano le fasi di generazione delle chiavi, cifratura e decifratura.
    - (10 punti) Sia (n=55, e=7) la chiave pubblica di Alice.
        i. Si calcoli la cifratura del messaggio m=7 per Alice, utilizzando un algoritmo a scelta tra left-to-right e right-to-left.
        ii. Si calcoli la chiave privata di Alice, utilizzando l'algoritmo di Euclide esteso.
    - (10 punti) Sia C la cifratura di un messaggio M con la chiave pubblica (n,e). Si definisca il bit $half_{n,e}(C)$ e si illustri come la conoscenza di tale bit possa essere sfruttata per attaccare il crittosistema RSA. Inoltre si analizzi la complessità dell'attacco.

4. (25 punti) Schema di Diffie-Hellman per l'accordo su chiavi.
    - (10 punti) Si descrivano ed analizzino gli algoritmi per la generazione dei parametri pubblici e per l'accordo sulla chiave.
    - (5 punti) E' possibile utilizzare p=17, g=2 come parametri pubblici? Si giustifichi la risposta.
    - (10 punti) Si descriva la generalizzazione dello schema per n partecipanti e se ne analizzi la sicurezza.