Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: B. Masucci

Appello del 31/01/2006

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
/20	/30	/30	/20	/100

1. (20 punti) Crittosistema di Vigenère.
   - (10 punti) Si consideri l'usuale corrispondenza tra l'alfabeto 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

     Sia "*gennaio*" la parola chiave:
     i. (5 punti) Cifrare il testo "sicurezza su reti";
     ii. (5 punti) Decifrare il testo "vvbiaaqxmgga";
   - (10 punti) Si supponga di intercettare un testo cifrato con Vigenère, contenente tre occorrenze della stessa stringa, a partire dalle posizioni 47, 1293 e 2301. Si deduca la lunghezza della chiave utilizzata per cifrare il testo, motivando la risposta.

2. (30 punti) Funzioni hash.

Si consideri la funzione hash H definita come segue:

Dato un messaggio $M= X_1X_2$ costituito da due blocchi di 56 bit e dato un valore iniziale H_0 di 64 bit, sia $H(M)=H_2$, dove $H_i = DES_{X_i}[H_{i-1}]\oplus H_{i-1}$, con i=1,2.

Mostrare come utilizzare la proprietà del complemento di DES per costruire un nuovo messaggio M' tale che H(M')=H(M).

- 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. (30 punti) Crittosistema RSA.
    - (5 punti) Descrivere le fasi di generazione delle chiavi, cifratura e decifratura.
    - (5 punti) Dimostrare che le operazioni di cifratura e decifratura sono una l'inversa dell'altra.
    - (5 punti) Sia n=33 un modulo RSA. Indicare, in ordine crescente, tutti i valori possibili per l'esponente pubblico "e", giustificando la risposta.
    - (5 punti) Per il terzo valore possibile di "e" determinato al punto precedente, trovare la corrispondente chiave privata "d" mediante l'algoritmo di Euclide esteso.
    - (10 punti) Analizzare la sicurezza di RSA contro un attacco del tipo chosen ciphertext.

4. (20 punti) Descrivere ed analizzare lo schema di Merkle per l'accordo su chiavi tra due partecipanti.
    - (5 punti) Descrivere l'algoritmo per la computazione di un puzzle da parte di Alice.
    - (5 punti) Descrivere ed analizzare l'algoritmo per la soluzione di un puzzle da parte di Bob.
    - (10 punti) Analizzare la sicurezza dello schema.