Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: B. Masucci

Appello del 26/02/2007

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	/30	/20	/25	/100

1. (25 punti) Alice e Bob hanno inventato un protocollo per scambiarsi messaggi su una rete insicura. Il protocollo è basato sull'idea del one-time pad, ma Alice e Bob non condividono alcuna chiave segreta. Per ogni messaggio Alice e Bob scelgono a caso una chiave R_A e R_B, rispettivamente. Supponendo che Alice voglia inviare in modo sicuro il messaggio M a Bob, il protocollo consiste nei seguenti tre passi:
   - Alice invia a Bob $X_1 = M \oplus R_A$
   - Bob invia ad Alice $X_2 = X_1 \oplus R_B$
   - Alice invia a Bob : $X_3 = X_2 \oplus R_A$

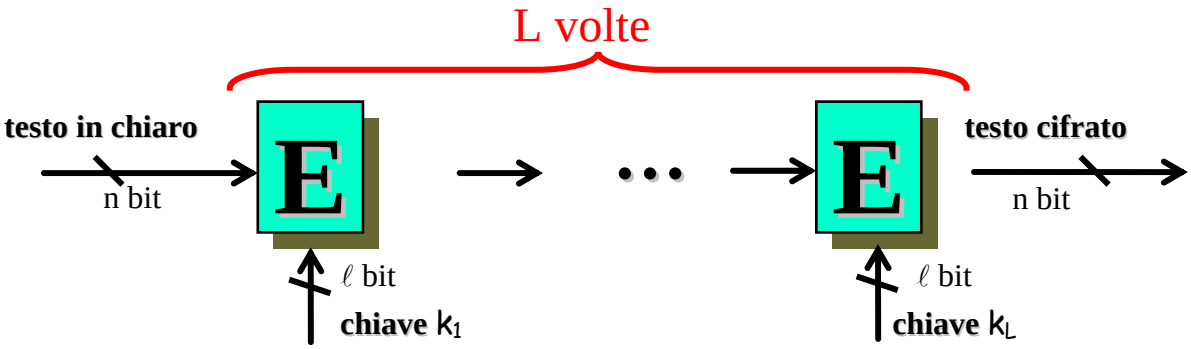
   a. (10 punti) Si mostri che Bob può decifrare il messaggio M.

   b. (15 punti) Si discuta la sicurezza di tale protocollo rispetto ad un attaccante che abbia intercettato tutte le comunicazioni tra Alice e Bob.

2. (30 punti) Crittosistema RSA.
   - (10 punti) Si descrivano le fasi di generazione delle chiavi, cifratura e decifratura. Inoltre, si mostri che le operazioni di cifratura e decifratura sono una l'inversa dell'altra.
   - (20 punti) Sia n=323 il modulo RSA di Alice.
     i. (10 punti) Si supponga che Oscar venga a conoscenza del valore $\Phi(n)=288$. Si illustri quali informazioni possono essere ricavate da Oscar, illustrando tutte le computazioni effettuate.
     ii. (10 punti) Sia e=35 l'esponente pubblico di Alice e sia C=23 un testo cifrato per Alice. Si mostri come Oscar sia in grado di risalire al testo in chiaro corrispondente, illustrando tutte le computazioni effettuate.

3. (20 punti) Schema di Diffie-Hellman per l'accordo su chiavi tra due partecipanti.
   - (10 punti) Descrivere ed analizzare gli algoritmi per la generazione dei parametri pubblici e per l'accordo sulla chiave.
   - (10 punti) Analizzare la sicurezza dello schema.

4. (25 punti) Sia E un cifrario a blocchi con taglia del blocco di n bit e lunghezza della chiave di ℓ bit.



- (15 punti) Si descriva l'attacco meet in the middle al cifrario E iterato L volte (si veda la figura) e si analizzi la complessità spazio/tempo dell'attacco.
- (5 punti) Data una coppia (x,y) di testo in chiaro e corrispondente cifrato, si calcoli il numero medio di chiavi $(k_1,\ldots,k_L)$ tali che $y=E_{k_L}(E_{k_{L-1}}(\ldots(E_{k_1}(x)))$.
- (5 punti) Si effettui la computazione descritta al punto precedente supponendo di avere in input t coppie $(x_1,y_1),\ldots(x_t,y_t)$ di testi in chiaro e corrispondenti cifrati.