Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: B. Masucci

Prova intercorso del 2/11/2005

Non è ammesso alcun materiale per la consultazione. Buon lavoro!

1	2	3	4	totale
/30	/20	/20	/20	/90

1. (30 punti) Considerare il seguente crittosistema: Data una stringa k di m caratteri ed un testo in chiaro in italiano 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} attraverso uno shift a destra di un posto (modulo 21, considerando l'alfabeto italiano).
   - Ad esempio, se k= CIAO e n=12, la chiave ottenuta è: CIAODLBPEMCQ.

   Il testo cifrato si ottiene effettuando la somma modulo 21 del testo in chiaro e della chiave costruita come sopra.
   Analizzare la sicurezza del crittosistema rispetto ad un ciphertext-only attack, spiegando in dettaglio i passi da effettuare per risalire al testo in chiaro.

2. (20 punti) Descrivere il funzionamento di un Linear Feedback Shift Register ed analizzarne la sicurezza rispetto ad un known plaintext attack.

3. (20 punti) Descrivere ed analizzare il DES doppio.
    - (5 punti) Descrivere il DES doppio.
    - (10 punti) Illustrare come rompere il DES doppio mediante un attacco di tipo known plaintext e analizzare la complessità (tempo, spazio) dell'attacco.
    - (5 punti) Determinare il numero di coppie necessarie affinché l'attacco abbia successo con probabilità prossima ad 1.

4. (20 punti) Crittosistema Blowfish.
    - (10 punti) Provare che la decifratura può essere effettuata applicando l'algoritmo di cifratura al testo cifrato con le chiavi schedulate in ordine inverso.
    - (10 punti) Data una coppia nota (testo in chiaro, testo cifrato) e supponendo che la chiave di cifratura (non nota) sia costituita da 14 word, quante cifrature deve effettuare un attaccante, nel caso peggiore, per determinare la chiave di cifratura? Giustificare la risposta.