Sicurezza nelle Reti

Appello del 7 Luglio 2006

Nome e Cognome_____**Matricola** _____

QUESITO 1 **PUNTI: 12 (5, 1, 2, 4)**

Sia W un borsellino elettronico che memorizza informazioni relative ai clienti, come nome, indirizzo e numero di carta di credito, ed esegue pagamenti per loro conto. Un cliente C viene identificato da W per mezzo di un PIN, un numero segreto su p bit condiviso tra C ed W. La Sia PKW la chiave pubblica del server W, su k bit, che si suppone pubblicamente nota.

Sia D la descrizione (una stringa di caratteri) della merce che C vuole acquistare, sia nota a W oltre che a C. Un possibile protocollo di autorizzazione dell'acquisto è costituito dai seguenti messaggi:

M1 $W \rightarrow C$: W, tid, D

M2 $C \rightarrow W$: C, E_W(tid, D, PIN)

dove tid è l'identificatore unico di transazione generato da W ed $E_X(m)$ denota la cifratura della quantità m con la chiave pubblica di X. Il candidato risponda alle seguenti domande motivando le risposte.

1. Il protocollo garantisce la confidenzialità della quantità PIN rispetto ad ciphertext-only attack? Si determini il tempo medio necessario per tale attacco nel caso che $k = 1024$, $p = 4$ ed il tempo necessario ad eseguire una cifratura/decifratura è di circa 50ms.

   SOLUZIONE. In M2 le quantità *tid* e *D* non sono segrete (lette in M1). Inoltre PKW è pubblica. Per cui si può fare una ricerca esaustiva sul PIN. Il tempo medio è $(50 \times 10^4)/2 = 250000$ ms = 250 s = 6 minuti e 10 secondi

2. Tale attacco può essere condotto off-line?

   SOLUZIONE. Si.

3. Tenendo conto della risposta al punto 2, il server W può attribuire il messaggio M2 al customer C?

   SOLUZIONE. NO.

4. Nel caso la risposta alla domanda 3 sia negativa, apportare una modifica al protocollo in modo da garantire l'autenticità del customer senza però assegnare alcuna coppia di chiavi publica-privata al customer.

   SOLUZIONE. Basta che il customer concateni un numero random di sua scelta alle quantità tid, D, PIN nel messaggio M2. Il numero random deve avere una lunghezza sufficiente da rendere praticamente impossibile un attacco esaustivo ai dati.

QUESITO 2 **PUNTI: 8 (5, 3)**

Con precisione matematica e proprietà di linguaggio, si definisca il *true random cipher* e ne discuta i problemi relativi ad una pratica realizzabilità.

SOLUZIONE. Vedere materiale didattico

QUESITO 3 **PUNTI: 12 (3, 3, 2, 4)**

1. Si spieghi con precisione matematica e proprietà di linguaggio quando un cifrario vene detto *sicuro dal punto di vista computazionale*.

   SOLUZIONE. Vedere materiale didattico.

2. Si definiscano i due attacchi: *known-plaintext attack* e *chosen-plaintext attack*.

   SOLUZIONE. Vedere materiale didattico**.**

Si consideri il cifrario a blocchi FEAL-*N* caratterizzato dai seguenti parametri: block size $n = 64$ bit , key size $k = 64$ e numero di round $N = 4, 6, 8, 16, 24, 32$. La Tabella 1 specifica la resistenza di FEAL a vari attacchi.

3. Si vuole garantire la confidenzialità delle informazioni per almeno un giorno rispetto ad un avversario capace di un known-plaintext attack. Si indichi quali cifrari sono da considerarsi insicuri in tal caso.

   SOLUZIONE. Si scarta FEAL-N per N uguale a 4, 6 ed 8. Gli altri cifrari possono essere utilizzati perché l'attacco più efficiente è di tipo chosen-plaintext attack ma l'avversario non è capace di questo tipo di attacco per ipotesi.

4. Si indichi quali cifrari sono da considerarsi insicuri nel caso che si voglia garantire la confidenzialità delle informazioni per almeno un mese rispetto ad un avversario che è capace di un chosen-plaintext attack *off-line*,[1] che dispone di hardware convenzionale (un PC ad esempio), e che riesce ad eseguire operazioni di cifratura e decifratura in 1 ms.

   SOLUZIONE. Si scarta FEAL 16 perché richiede circa 8 Gbytes di memoria per memorizzare offline i chosen pairs ed impiega circa 106 secondi (12 gg) per condurre l'attacco.

Tabella 1. *Attacchi a FEAL. LC sta per linear cryptonalysis e DC sta per differential cryptoanalysis***.**

attack method	data complexity		storage complexity	processing complexity
	known	chosen		
FEAL-4 – LC	5	—	30 Kbytes	6 minutes
FEAL-6 – LC	100	—	100 Kbytes	40 minutes
FEAL-8 – LC FEAL-8 – DC	2^{24}	2^7 pairs	280 Kbytes	10 minutes 2 minutes
FEAL-16 – DC	—	2^{29} pairs		2^{30} operations
FEAL-24 – DC	—	2^{45} pairs		2^{46} operations
FEAL-32 – DC	—	2^{66} pairs		2^{67} operations

[1] L'avversario accumula i chosen pair necessari e poi li utilizza come dati dell'algoritmo di crittoanalisi.