CRITTOGRAFIA 2015/16 – Appello del 30 maggio 2016

Nome e Cognome:

Matricola:

Esercizio 1 – RSA [14 punti]

1. **Spiegare** in cosa consiste il cifrario RSA, **definendone** i parametri e **indicando** le operazioni eseguite per ottenerli e la loro complessità computazionale.
2. **Dimostrare** che il cifrario è corretto per qualunque messaggio m.
3. **Indicare** in quali intervalli, in ordine di grandezza, devono essere scelti i parametri p e q.

Esercizio 2 – Cifrari a composizione di blocchi [8 punti]

Si consideri un cifrario simmetrico a blocchi. Nel metodo FSM (Fischer Spiffy Mixer) ogni blocco m_i del messaggio in chiaro viene cifrato come

$$c_i = m_{i-1} \oplus C(m_i \oplus c_{i-1},k), \quad i \geq 1$$

usando due sequenze di inizializzazione fissate (e pubbliche) m_0 e c_0.

1. **Descrivere** come eseguire la decifrazione di un blocco.
2. Nel caso in cui il blocco di crittogramma c_i sia danneggiato, quali blocchi di testo in chiaro diventano indecifrabili?

Esercizio 3 – Firma digitale [8 punti]

Descrivere un protocollo di firma digitale resistente agli attacchi di tipo *man-in-the-middle*.

Esercizio 4 – [1 punto]

Decifrare

LOCE LOCE LOCE

LOCE LOCE LOCE LOCE LOCE LOCE LOCE LOCE LOCE

[***Suggerimento***: 5, 6]

CRITTOGRAFIA 2015/16 – Appello del 21 giugno 2016

Nome e Cognome:

Matricola:

Esercizio 1 – Cifrari [12 punti]

Discutere in massimo trenta righe quali sono le differenze d'impiego tra i tre cifrari One-Time Pad, AES e RSA, **giustificando** le affermazioni fatte.

Esercizio 2 – Scambio di chiavi [12 punti]

L'algoritmo DH per lo scambio pubblico di chiavi è basato sull'uso di un primo p e di un generatore g di Z^*p.

1. **Descrivere** l'algoritmo e sviluppare un esempio numerico utilizzando il numero primo p = 11 e il generatore g = 7 di Z^*_{11} .
2. **Descrivere** un attacco di tipo *man-in-the-middle* al protocollo DH.

Esercizio 3 – RSA [6 punti]

Si supponga che Eve intercetti un crittogramma $c = m^e \bmod n$ diretto ad Alice. Si supponga inoltre che Alice sia disposta a decifrare per Eve qualsiasi crittogramma c', a patto che c' sia diverso da c.

Descrivere come Eve possa decifrare m in tempo polinomiale, richiedendo ad Alice la decifrazione del crittogramma $c' = c\, x^e$, dove $x < n$ è un intero casuale, co-primo con n.

CRITTOGRAFIA 2015/16 – Appello del 14 luglio 2016

Nome e Cognome:

Matricola:

Esercizio 1 – Cifrari perfetti [12 punti]

1. **Definire** i cifrari perfetti, e **spiegare** a parole il significato di tale definizione.
2. **Definire** il cifrario One-Time Pad e le assunzioni standard su di esso.
3. **Dimostrare** che il cifrario del punto 2 è perfetto.
4. **Spiegare** se la crittoanalisi statistica può essere usata per attaccare One-Time Pad

Esercizio 2 – Cifrari storici [6 punti]

In riferimento ai cifrari a griglia;

1. spiegare in cosa consiste un tale cifrario;
2. dimostrare quante chiavi diverse si possono costruire per una griglia $q \times q$;
3. discutere (senza pretesa di profondità) la propria opinione sulla possibilità di un attacco statistico per cifrari a griglia.

Esercizio 3 – Crittografia ellittica [12 punti]

Impiegando una curva ellittica $E_p(a,b)$ su un campo finito:

1. **Spiegare** come si esegue in modo efficiente la moltiplicazione di un punto P per una costante intera k.
2. **Spiegare** cosa si intende per "logaritmo discreto" (se esiste) di un punto R in base P.
3. **Descrivere** un algoritmo di scambio di chiavi basato sulla crittografia ellittica e **spiegare** perché può ritenersi sicuro.

CRITTOGRAFIA 2015/16 – Appello del 7 settembre 2016

Nome:

Cognome:

Matricola:

Esercizio 1 – Crittografia ellittica [12 punti]

Impiegando una curva ellittica $E_p(a,b)$ su un campo finito:

1. **Descrivere** l'algoritmo di Koblitz per trasformare un messaggio *m,* codificato come numero intero, in un punto di una curva ellittica prima.
2. **Spiegare** cosa si intende per "logaritmo discreto" (se esiste) di un punto *R* in base *P*.
3. **Descrivere** un algoritmo di scambio di messaggi cifrati e **spiegare** perché può ritenersi sicuro.

Esercizio 2 – Identificazione [10 punti]

Indicare un protocollo di identificazione basato su un protocollo Zero Knowledge e **spiegare** vantaggi e svantaggi che un tale protocollo offre rispetto a uno basato su un cifrario a chiave pubblica.

Esercizio 3 – RSA [8 punti]

1. **Spiegare** perché nel cifrario RSA il parametro **e** deve essere scelto primo con $\Phi(n)$.
2. **Spiegare** se nel cifrario RSA la scelta dei parametri **p, q** tale che sia $|p-q| = \Theta((\log n)^2)$ è da considerarsi opportuna.