CRITTOGRAFIA 2013/14 – Appello del 10 gennaio 2014

Nome:

Cognome:

Matricola:

Esercizio 1 – Cifrari storici [8 punti]

Definire la crittoanalisi statistica e **spiegare** se e come essa possa essere impiegata nell'attacco ai cifrari:

1. di Cesare;
2. di de Vigenère;
3. One-time pad.

Esercizio 2 – Cifrari perfetti [8 punti]

1. **Definire** i cifrari perfetti e **spiegare a parole** il significato di tale definizione.
2. **Dimostrare** che in un cifrario perfetto il numero delle chiavi deve essere maggiore o uguale al numero dei messaggi possibili.

Esercizio 3 – RSA [8 punti]

Si consideri il cifrario RSA con chiave pubblica $n = 235$, $e = 11$.

1. **Cifrare** il messaggio m composto dalle due cifre meno significative del proprio numero di matricola (se le due cifre sono < 10, aggiungere 23).
2. **Forzare** il cifrario trovando p, q, d.
3. **Decifrare** il crittogramma $c = 200$.

Riportare esplicitamente tutte le operazioni aritmetiche eseguite (utilizzare l'algoritmo di Euclide Esteso per il calcolo dell'inverso in modulo, e il metodo delle quadrature successive per gli elevamenti a potenza).

Esercizio 4 – Firma digitale [6 punti]

Spiegare in cosa consiste un certificato digitale e perché tali certificati sono stati introdotti.

CRITTOGRAFIA 2013/14 – Appello del 28 gennaio 2014

Nome:

Cognome:

Matricola:

Esercizio 1 – Scambio di chiavi [9 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. Scelti $\boldsymbol{p = 11}$ e $\boldsymbol{g = 6}$:

1. **Verificare** che 6 è un generatore di Z^*_{11};
2. Presi due interi x, y come scelte casuali di due partner che devono costruire una chiave comune, **indicare** come procede l'algoritmo per questi due valori e quale chiave si costruisce;
3. **Spiegare** per quale motivo l'algoritmo è sicuro (ovviamente per valori di p, g molto grandi).
4. **Descrivere** un attacco di tipo *man-in-the-middle* al protocollo DH.

Esercizio 2 – RSA [8 punti]

Considerando il cifrario RSA e i suoi parametri p, q, n:
1. Dimostrare che tale cifrario è corretto per qualunque messaggio m.
2. Spiegare perché si deve scegliere $m < n$.
3. Spiegare in quali intervalli, in ordine di grandezza, devono essere scelti i parametri p e q.

Esercizio 3 – Numeri primi [7 punti]

Applicando l'algoritmo di Miller e Rabin, individuare un numero N primo di tre cifre decimali con probabilità di errore < 1/10, spiegando il procedimento eseguito.
Si ricordi che dati un numero N e un intero arbitrario y, $2 \le y \le N-1$, se N è un numero primo, devono essere veri i due predicati:

P1: $\text{mcd}(N,y) = 1$

P2: ($y^z \bmod N = 1$) or (esiste un valore i, $0 \le i \le w-1$, tale che $y^{2^i z} \bmod N = -1$)

dove z e w sono definiti da $N-1 = z\,2^w$ con z dispari.

Esercizio 4 – Crittografia ellittica [6 punti]

Impiegando una curva ellittica $Eq(a,b)$ su un campo finito, descrivere un algoritmo per lo scambio di messaggi cifrati e spiegare perché può ritenersi sicuro.

CRITTOGRAFIA 2013/14 – Appello del 4 giugno 2014

Nome:

Cognome:

Matricola:

Esercizio 1 – Scambio di chiavi [8 punti]

Illustrare brevemente il protocollo BB84 per lo scambio di chiavi segrete basato sulla trasmissione di fotoni polarizzati e **spiegare** perché può ritenersi sicuro.

Esercizio 2 – RSA [7 punti]

Spiegare se nel cifrario RSA la scelta dei parametri **p, q** tale che sia $|\mathbf{p-q}| = \Theta((\log n)^2)$ è da considerarsi opportuna.

Esercizio 3 – Firma digitale [7 punti]

Descrivere un attacco attivo al protocollo di firma digitale in cui il messsaggio è cifrato e firmato in hash.

Esercizio 4 – Chiave pubblica [8 punti]

Il cifrario El Gamal utilizza una coppia pubblica *p, g*, ove *p* è un numero primo e *g* è un suo generatore. Ogni utente U sceglie come **chiave privata** un intero random *x* tra 2 e *p*-2, e **pubblica la chiave** $y = g^x \bmod p$. I blocchi *m* del messaggio sono interi < *p*. L'invio di un messaggio cifrato a U avviene scegliendo un intero random *k* tra 2 e *p-1* e inviando la coppia $< c = g^k \bmod p,\ d = y^k m \bmod p >$. La decifrazione avviene calcolando $(d / c^x) \bmod p = m$.

Presa la coppia *p = 43, g = 3* (infatti 3 è un generatore di 43), U sceglie *x = 7*.

1. **Calcolare** la chiave pubblica di U.
2. **Indicare** i calcoli eseguiti per l'invio a U e per la decifrazione del messaggio composto dalle due cifre meno significative del proprio numero di matricola, prese modulo 43.

CRITTOGRAFIA 2013/14 – Appello del 23 giugno 2014

Nome:

Cognome:

Matricola:

Esercizio 1 – Crittografia ellittica [8 punti]

Si consideri una curva ellittica $E_p(a,b)$ su un campo finite.

1. **Spiegare** cosa si intende per "logaritmo discreto" (se esiste) di un punto R in base P.
2. **Descrivere** un algoritmo di scambio di chiavi basato sulla crittografia ellittica e **spiegare** perché può ritenersi sicuro.

Esercizio 2 – Complessità in algebra [6 punti]

Dato un intero n **definire** la funzione di Eulero $\Phi(n)$, **indicare** se è noto un algoritmo efficiente per calcolarla e **spiegare** in termini matematici quale implicazione avrebbe questo algoritmo sui cifrari DES e RSA e sui protocolli di firma.

Esercizio 3 – Firma digitale [6 punti]

Descrivere un protocollo di firma digitale che **non** preveda la firma diretta del messaggio.

Esercizio 4 – RSA [10 punti]

1. **Spiegare** in cosa consiste il cifrario RSA, **definendone** tutti i parametri e **indicando** esplicitamente le operazioni eseguite per ottenerli e la loro complessità computazionale.
2. **Dimostrare** che tale cifrario è corretto per qualunque messaggio m.
3. **Darne** un esempio di applicazione impiegando parametri numerici molto piccoli per cifrare il messaggio costituito dalle due cifre meno significative del proprio numero di matricola.

CRITTOGRAFIA 2013/14 – Appello dell'11 luglio 2014

Nome:

Cognome:

Matricola:

Esercizio 1 – Numeri primi [14 punti]

1. **Descrivere** l'algoritmo di Miller e Rabin per il test di primalità e **discuterne** la complessità.
2. Applicando l'algoritmo di Miller e Rabin, **individuare** un numero N primo di tre cifre decimali con probabilità di errore < 1/15, **spiegando** il procedimento eseguito.

Si ricordi che dati un numero N e un intero arbitrario y, $2 \leq y \leq N-1$, se N è un numero primo, devono essere veri i due predicati:

P1: $\text{mcd}(N,y) = 1$

P2: ($y^z \bmod N = 1$) or (esiste un valore i, $0 \leq i \leq w-1$, tale che $y^{2^i z} \bmod N = -1$)

dove z e w sono definiti da $N-1 = z\,2^w$ con z dispari.

Esercizio 2 – Cifrari perfetti [8 punti]

Dimostrare che il cifrario *One-Time Pad* è un cifrario perfetto.

Esercizio 3 – Identificazione [8 punti]

1. **Descrivere** un protocollo di identificazione su canale sicuro.
2. **Descrivere** un protocollo di identificazione su canale insicuro.

CRITTOGRAFIA 2013/14 – Appello del 10 settembre 2014

Nome:

Cognome:

Matricola:

Esercizio 1 – Complessità in algebra [6 punti]

Dato un intero n prodotto di due numeri primi, **dimostrare** che il calcolo della funzione di Eulero $\Phi(n)$ e la fattorizzazione di n sono problemi computazionalmente equivalenti.

Esercizio 2 – RSA [14 punti]
I parametri del cifrario RSA, nonché il suo impiego, sono presi come noti. Domande:
1. **Dimostrare** che il cifrario é corretto (cioè che un messaggio cifrato viene decifrato correttamente);
2. **Spiegare** come il cifrario possa essere impiegato nella firma digitale **indicando un esempio numerico completo a scelta** (si ponga $m > 64$, e come funzione hash $h(x)$ si prendano i bit in posizione 1, 3 e 5 della rappresentazione binaria di x).

Esercizio 3 – Crittografia ellittica [10 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.