CRITTOGRAFIA 2014/15 – Appello del 13 gennaio 2015

Nome:

Cognome:

Matricola:

Esercizio 1 – Crittografia ellittica [9 punti]

1. **Descrivere** l'algoritmo di Koblitz per trasformare un messaggio m, codificato come numero intero, in un punto di una curva ellittica prima.
2. **Trasformare** il messaggio $m = 5$ in un punto della curva prima $E_{67}(1,1)$.

Esercizio 2 – Cifrari perfetti [9 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 [12 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. RSA è un cifrario a blocchi: **indicare** come devono essere scelte le dimensioni dei blocchi.
3. **Dare** un esempio di applicazione impiegando parametri numerici molto piccoli per cifrare il messaggio m costituito dalle due cifre centrali del proprio numero di matricola (se $m < 3$, aggiungere 8).

CRITTOGRAFIA 2014/15 – Appello del 3 febbraio 2015

Nome:

Cognome:

Matricola:

Esercizio 1 – Crittografia ellittica [14 punti]

Impiegando una curva ellittica prima su un campo finito:

1. **Spiegare** come trasformare un numero intero in un punto della curva.
2. **Descrivere** un algoritmo di scambio di messaggi cifrati e **spiegare** perché può ritenersi sicuro.
3. **Trasformare** il messaggio $m = 5$ in un punto della curva prima $E_{23}(1,1)$.

Esercizio 2 – RSA [12 punti]

Sia M il proprio numero di matricola, e sia M' il numero composto dalla prima e dall'ultima cifra di M. Siano quindi p il più piccolo numero primo maggiore di M', e q il numero primo successivo a p.

1. **Costruire** i parametri di un cifrario RSA impiegando p e q scelti sopra. Impiegare l'algoritmo di Euclide Esteso per il calcolo della chiave segreta indicando i calcoli eseguiti.
2. **Mostrare** come i valori scelti per p e q rendano tale cifrario facilmente attaccabile **indicando i calcoli** da eseguire per l'attacco.

Esercizio 3 – Firma digitale [4 punti]

Descrivere un attacco di tipo *man-in-the-middle* ai protocolli di firma digitale che utilizzano cifrari asimmetrici.

CRITTOGRAFIA 2014/15 – Appello del 3 giugno 2015

Nome:

Cognome:

Matricola:

Esercizio 1 – Cifrari storici [10 punti]

Usando il metodo di Vigenère, **cifrare** il messaggio CRITTOGRAFIA impiegando come chiave le prime 4 lettere del proprio cognome. **Spiegare** inoltre come tale cifrario possa essere attaccato.

Si ricorda che la tabella di Vigenère è la seguente:

```
A B C … X Y Z
B C D … Y Z A
… …       …
Z A B … W X Y
```

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 – Firma digitale [10 punti]

Due utenti A, B si scambiano messaggi in chiaro ma firmati in hash con RSA. **Spiegare**:

1. come si costruiscono i parametri necessari alla firma indicando la complessità delle operazioni;
2. quale implicazione avrebbe sulla firma la scoperta di un algoritmo polinomiale per il calcolo della funzione di Eulero di un numero arbitrario.

CRITTOGRAFIA 2014/15 – Appello del 19 giugno 2015

Nome:

Cognome:

Matricola:

Esercizio 1 – Numeri primi [10 punti]

Applicando l'algoritmo di Miller e Rabin, individuare un numero N primo di tre cifre decimali con probabilità di errore minore di 1/50, spiegando il procedimento eseguito.

Esercizio 2 – 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.

Esercizio 3 – Firma digitale [10 punti]

Nel classico schema di firma che impiega un cifrario asimmetrico le funzioni di cifratura e decifrazione devono essere commutative.

1. **Spiegarne** il motivo.
2. **Indicare** un protocollo di firma in cui è utilizzata questa caratteristica.

CRITTOGRAFIA 2014/15 – Appello del 7 luglio 2015

Nome:

Cognome:

Matricola:

Esercizio 1 – Casualità [8 punti]

Dare la definizione di sequenza casuale secondo Kolmogorov e **illustrarne** il significato.

Esercizio 2 – Chiave pubblica [12 punti]

Il cifrario a chiave pubblica El Gamal utilizza una coppia **pubblica** p, g, ove p è un numero primo e $g < p$ è un suo generatore. Ogni utente U sceglie un intero random x tra 2 e p-2, e pone:

chiave privata = x,
chiave pubblica = $y = g^x \bmod p$.

L'invio verso U di un blocco b di messaggio, con $b < p$, avviene scegliendo un intero random k tra 2 e p-2 e inviando la coppia: $< c = g^k \bmod p,\ d = y^k\, b \bmod p >$.
U decifra il blocco calcolando $(d / c^x) \bmod p = b$.

1. **Dimostrare** che il cifrario funziona, cioè i messaggi sono cifrati e decifrati correttamente
2. **Spiegare** perché il cifrario può ritenersi sicuro
3. **Spiegare** perché il suo impiego è ragionevole dal punto di vista della complessità di calcolo.
4. Presa la coppia $p = 17,\ g = 3$, U sceglie $x = 6$. **Calcolare** la chiave pubblica di U e **decifrare** il testo cifrato < 7, 6 >.

Esercizio 3 – Autenticazione e firma [10 punti]

Spiegare che proprietà devono possedere le funzione hash one-way, e perché tali funzioni sono importanti nei protocolli di autenticazione e di firma.

CRITTOGRAFIA 2014/15 – Appello dell'11 settembre 2015

Nome:

Cognome:

Matricola:

Esercizio 1 – Firma digitale [8 punti]

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

Esercizio 2 – Algoritmi per crittografia [10 punti]

L'algoritmo di Euclide Esteso EE è così definito:

```
EE(a, b):
if  (b == 0) return (a, 1, 0)
else  {
        (d', x', y') = EE(b, a mod b);
        (d, x, y) = (d', y', x'-(a/b)y');
        return (d, x, y)
}
```

1. **Indicare** quale problema risolve EE, cioè cosa rappresentano i valori di d, x, y all'uscita.
2. **Dimostrare** perché e come EE può essere impiegato per calcolare un inverso in modulo per valori opportuni dei parametri.
3. **Dare** un esempio a piacere di sua applicazione.

Esercizio 3 – Cifrari perfetti [12 punti]

1. **Definire** il cifrario One-Time Pad e le assunzioni standard su di esso.
2. **Dimostrare** che il cifrario One-Time Pad è perfetto.
3. **Dare** un esempio a piacere di sua applicazione.

CRITTOGRAFIA 2014/15 – Appello del 12 gennaio 2016

Nome:

Cognome:

Matricola:

Esercizio 1 – Crittografia ellittica [14 punti]

Impiegando una curva ellittica prima su un campo finito:

1. **Spiegare** come trasformare un numero intero in un punto della curva.
2. **Trasformare** il messaggio $m = 8$ in un punto della curva prima $E_{23}(1,1)$.
3. **Descrivere** un algoritmo di scambio di messaggi cifrati e **spiegare** perché può ritenersi sicuro.

Esercizio 2 – Scambio di chiavi [10 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 **svilupparne** un esempio numerico utilizzando il numero primo $\boldsymbol{p = 13}$ e il generatore $\boldsymbol{g = 7}$ di Z^*_p
2. **Descrivere** un attacco di tipo *man-in-the-middle* al protocollo DH.

Esercizio 3 – One-time Pad [6 punti]

Nel cifrario One-Time Pad si consideri una coppia arbitraria messaggio/crittogramma m, c di n bit. **Spiegare** quanto vale la probabilità $P(M=m, C=c)$ (**NOTA**: questa è la probabilità dell'intersezione degli eventi, non la probabilità condizionale).

CRITTOGRAFIA 2014/15 – Appello del 2 febbraio 2016

Nome:

Cognome:

Matricola:

Esercizio 1 – Cifrari storici [10 punti]

Si deve cifrare il messaggio APPELLODIFEBBRAIO impiegando come chiave una permutazione arbitraria e segreta delle 26 lettere dell'alfabeto.

1. **Mostrare** la permutazione scelta e il crittogramma ottenuto.
2. **Calcolare** il numero di prove necessario per condurre un attacco esauriente sulle chiavi.
3. **Discutere** la possibilità di un attacco più efficiente confrontandolo con quello del punto 2.

Esercizio 2 – Scambio di chiavi 1 [10 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 $\boldsymbol{p = 13}$ e $\boldsymbol{g = 6}$:

1. **Verificare** che 6 è un generatore di Z^*_{13};
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 3 – Scambio di chiavi 2 [10 punti]

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