CRITTOGRAFIA 2021/22 – Appello del 20 luglio 2022 - compito 1

Nome e Cognome:

Matricola:

Esercizio 1 – Protocolli [6 punti]

Descrivere il protocollo SSL, con particolare riferimento alla fase di *Handshake.*

Esercizio 2 – Crittografia ellittica [14 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. Sia k l'intero formato dalla prima e dalla terza cifra del proprio numero di matricola. Dato un punto P della curva, con quante operazioni (raddoppi e somme di punti) è possibile calcolare il punto $Q = k\,P$? **Mostrare** le operazioni che devono essere eseguite (senza calcolare i risultati).
3. **Descrivere** l'algoritmo di Koblitz e **sviluppare** un esempio di applicazione per trasformare il messaggio m corrispondente alla cifra meno significativa del proprio numero di matricola in un punto della curva ellittica E_{23} (1,1). Se $m > 5$, si ponga $m = 5$. Se $m < 3$, si ponga $m = 4$. Si assegni ad h il valore 3.

Esercizio 3 – Cifrari perfetti [10 punti]

1. **Definire** i cifrari perfetti, e **spiegare** a parole il significato di tale definizione.
2. **Dimostrare** il Teorema di Shannon.
3. **Spiegare** se si può usare un attacco esauriente sulle chiavi per attaccare il cifrario One-Time Pad.

CRITTOGRAFIA 2021/22 – Appello del 20 luglio 2022 - compito 2

Nome e Cognome:

Matricola:

Esercizio 1 – Sequenze casuali [6 punti]

Dare la definizione di sequenza casuale secondo Kolmogorov, **illustrandone** il significato, e **dimostrare** l'esistenza di sequenze casuali secondo Kolmogorov di ogni lunghezza *n*.

Esercizio 2 – Scambio di chiavi su curve ellittiche [14 punti]

1. **Descrivere** il protocollo DH su curve ellittiche per lo scambio di chiavi segrete.
2. **Spiegare** per quale motivo il protocollo può ritenersi sicuro.
3. **Descrivere** un attacco attivo al protocollo.
4. **Proporre** un'estensione del protocollo che permetta a tre utenti (Alice, Bob e Charlie) di generare e scambiarsi una chiave segreta.

Esercizio 3 – Algoritmi per la crittografia [10 punti]

L'algoritmo di Euclide Esteso EE è così definito:

```
Function 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** come EE possa essere impiegato per calcolare un inverso in modulo per valori opportuni dei parametri **indicando i calcoli** eseguiti in un esempio numerico.
3. **Indicare** un protocollo crittografico in cui EE è utilizzato.

CRITTOGRAFIA 2021/22 – Appello del 20 luglio 2022 - compito 3

Nome e Cognome:

Matricola:

Esercizio 1 – RSA [14 punti]

I parametri del cifrario RSA, nonché il suo impiego, sono noti. Domande:

1. RSA è un cifrario a blocchi: **spiegarne** il motivo **indicando** come devono essere scelte le dimensioni dei blocchi;
2. **dimostrare** che il cifrario funziona, cioè i messaggi sono cifrati e decifrati correttamente;
3. **descrivere** un protocollo di **identificazione** e un protocollo di **firma digitale** che utilizzano il cifrario RSA.

Esercizio 2 – Scambio di chiavi [10 punti]

1. **Illustrare** il protocollo BB84 per lo scambio di chiavi segrete basato sulla trasmissione di fotoni polarizzati e **spiegare** perché può ritenersi sicuro.
2. **Darne** un breve esempio di applicazione (in **assenza** di crittoanalista sul canale)
   - si usi la sequenza di 16 bit ottenuta trasformando ordinatamente in binario le quattro cifre decimali meno significative del proprio numero di matricola
   - si scelgano a caso le basi per imporre, intercettare e per misurare la polarizzazione dei fotoni
   - si indichino con precisione tutti i passi del protocollo

Esercizio 3 – Moneta elettronica [6 punti]

Descrivere il processo di validazione tramite *mining* delle transazioni Bitcoin.

CRITTOGRAFIA 2021/22 – Appello del 15 giugno 2022 - compito 1

Nome e Cognome:

Matricola:

Esercizio 1 – Scambio di chiavi [12 punti]

1. **Illustrare** il protocollo BB84 per lo scambio di chiavi segrete basato sulla trasmissione di fotoni polarizzati e **spiegare** perché può ritenersi sicuro.
2. **Darne** un breve esempio di applicazione (in **presenza** di crittoanalista sul canale)
   - si usi la sequenza di 16 bit ottenuta trasformando ordinatamente in binario le quattro cifre decimali meno significative del proprio numero di matricola
   - si scelgano a caso le basi per imporre, intercettare e per misurare la polarizzazione dei fotoni
   - si indichino con precisione tutti i passi del protocollo

Esercizio 2 – Crittografia ellittica [12 punti]

1. **Calcolare** l'ordine della curva ellittica prima $E_{13}(a,b)$ ottenuta scegliendo come coefficienti a e b la prima e la quarta cifra del proprio numero di matricola.
2. La curva definisce un gruppo abeliano?
3. **Descrivere** un algoritmo di scambio di chiavi basato sulla crittografia ellittica e **discuterne** la sicurezza.

Esercizio 3 – Funzioni hash e autenticazione di messaggi [6 punti]

1. **Spiegare** che proprietà devono possedere le funzioni *hash one-way*
2. **Descrivere** un protocollo di autenticazione che utilizza funzioni hash crittografiche e discuterne la sicurezza

CRITTOGRAFIA 2021/22 – Appello del 15 giugno 2022 - compito 2

Nome e 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. **Sviluppare** un esempio di applicazione dell'algoritmo per trasformare un messaggio *m* scelto a piacere nell'intervallo [5,9] in un punto della curva ellittica $E_{19}(1,1)$.
3. **Descrivere** un algoritmo per lo scambio di messaggi cifrati su curve ellittiche e **dimostrarne** la correttezza.

Esercizio 2 - RSA [10 punti]

1. **Dare** un esempio di applicazione del cifrario RSA impiegando parametri numerici molto piccoli per cifrare il messaggio costituito dalle due cifre centrali del proprio numero di matricola, se le due cifre sono minori di 10, aggiungere 33. *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).*
2. **Mostrare** come sia possibile attaccare il cifrario RSA quando più utenti scelgono lo stesso valore di **e**.

Esercizio 3 – Funzioni hash e firma digitale [9 punti]

1. **Spiegare** che proprietà devono possedere le funzioni *hash one-way*
2. **Descrivere** un protocollo di firma digitale che utilizza funzioni hash crittografiche e discuterne la sicurezza
3. **Descrivere** dove intervengono le funzioni hash nell'ambito della valuta digitale bitcoin.