CR410 AA11/12 (Crittografia 1)

**ESAME DI METÀ SEMESTRE** **Roma, 4 Aprile 2012.**

1. Dato il numero binario $n = (1111110101)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)
2. Determinare una stima per il numero di operazioni bit necessarie per calcolare $[\sqrt{k^k \bmod T}]$ dove $T \leq k^3$.
3. Trovare un valore di $n$ intero per cui la congruenza $X^6 \equiv 1 \bmod n$ ha esattamente 36 soluzioni modulo $n$?
4. Mostrare che le moltiplicazioni nellanello quoziente $\mathbf{Z}/6\mathbf{Z}[x]/(x^d)$ si possono calcolare in $O(d^2)$ operazioni bit mentre le addizioni in $O(d)$ operazioni bit.
5. Dopo aver spiegato il funzionamento dell'algoritmo di Euclide per il calcolo dell'identità di Bezout tra due interi, lo si applichi per calcolare l'identità di Bezout tra 27 e 63.
6. Fornire una stima per probabilità che un intero composto $n \leq 10^{50}$ privo di fattori primi minori di 101 sia dichiarato primo da 10 iterazioni del test di Miller Rabin
7. Dopo aver definito la nozione di numeri di Carmichael ed averne elencato alcune delle proprietà findamentali, si dimostri che 8911 è un numero di Carmichael.
8. Calcololare il seguente simbolo di Jacobi senza fattorizzare: $\left(\frac{232}{919}\right)$.
9. Spiegare nei dettagli il funzionamento del crittosistema RSA e si dia un esempio di una sua implementazione.

**ESAME DI FINE SEMESTRE** **Roma, 28 Maggio, 2012.**

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:

   a. E' vero che tutte le curve ellittiche sono non singolari?
   b. Fornire un esempio di una curva ellittica su un campo finito con gruppo dei punti razionali non ciclico.
   c. Determinare le radici primitive (i.e. generatori) in $\mathbf{F}_2[\alpha]$ dove $\alpha^4 = 1 + \alpha$.
   d. E' vero che in $\mathbf{F}_q[X]$ esistono polinomi irriducibili di ogni grado?
2. Dopo aver definito la nozione di polinomio primitivo, calcolare la probabilità che un polinomio irriducibile di grado 8 su $\mathbf{F}_7$ sia primitivo.
3. Dimostrare che un polinomio monico, riducibile e senza fattori quadratici di grado 5 in $\mathbf{F}_q[X]$ è un fattore di $X^{q^{12}} - X$.
4. Spiegare il funzionamento del Crittosistema ElGamal fornendo un esempio esplicito su un campo con 13 elementi.
5. Dopo averne spiegato il funzionamento, implementare uno scambio chiavi Diffie–Hellmann in un campo finito con 32 elementi.
6. Spiegare la rilevanza del metodo Baby-Steps-Giant-Steps nella teoria delle curve ellittiche su campi finiti.
7. Sia $E : y^2 = x^3 - x$. Determinare la struttura del gruppo $E(\mathbf{F}_7)$ .
8. Supponiamo $\mathbf{F}_4 = \mathbf{F}_2[\xi], \xi^2 = 1 + \xi$. Determinare il numero di punti su un campo con $2^{100}$ elementi della curva ellittica su $\mathbf{F}_4$

$$E : y^2 + y = x^3 + \xi$$

9. Scrivere e dimostrare le formule per la duplicazione di un punto (finito) su un curva ellittica in un campo finito con caratteristica maggiore di 3.

**APPELLO A** **Roma, 5 Giugno, 2012.**

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:
   a. E' vero che l'algoritmo Pohlig–Hellman si applica a qualsiasi gruppo finito ciclico?
   b. Quale è la probabilità che dati $(x_1, \ldots, x_{100}) \in (\mathbf{Z}/500\mathbf{Z}^{100})$ ci siano $i \neq j$ tali che $x_i = x_j$?
   c. Che differenza c'è tra polinomi irriducibili e polinomi primitivi?
   d. E' vero che in $\mathbf{F}_p[X]$ due polinomi di grado 30 si moltiplicano in $O(\log^2 p)$ operazioni bit?
2. Descrivere due algoritmi per il calcolo del massimo comun divisore di interi, determinarne la complessità e sfruttarli per calcolare con entrambi $\mathrm{MCD}(75, 42)$.
3. Dopo aver definito i simboli di Jacobi e di Legendre dimostrare che se $p$ e $q$ sono numeri primi tali che $q \equiv 5 \bmod 4p$ e $p \equiv 2 \bmod 5$, allora il simbolo di Legendre $\left(\frac{p}{q}\right) = -1$.
4. Mostrare che se $n$ è un modulo RSA di cui si conosce il valore di $\varphi(n)$, allora è possibile determinare efficientemente i fattori primi di $n$. Come si può utilizzare questa informazione per decifrare messaggi cifrati con RSA?
5. Descritto l'algoritmo di Miller Rabin per verificare la primalità di un intero, stimarne la probabilità d'errore quando è applicato con 10 iterazioni su interi con 1000 cifre decimali.
6. Descrivere brevemente tutti gli algoritmi crittografici che basano la propria sicurezza sul problema del logaritmo discreto.
7. Determinare tutti i sottocampi di $\mathbf{F}_{7^{50}}$ che contengono un sottocampo con 49 elementi.
8. Supponiamo $\mathbf{F}_4 = \mathbf{F}_2[\xi], \xi^2 = 1 + \xi$. Determinare il numero di punti su un campo con $2^{12}$ elementi della curva ellittica su $\mathbf{F}_4$

$$E : y^2 + \xi y = x^3 + \xi$$

9. Descrivere il gruppo $E(\mathbf{F}_5)$ dove $E$ è la curva ellittica definita da $y^2 = x^3 - x$.

**APPELLO B** **Roma, 26 Giugno, 2012.**

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:
   a. E' vero che se $E$ è una curva ellittica definita su $\mathbf{F}_3$, allora si può agevolmente calcolare $E(\mathbf{F}_{3^{100}})$?
   b. E' vero che se $p - 1$ ha soltanto fattori piccoli allora i logaritmi discreti in $\mathbf{F}_p$ si calcolano efficientemente?
   c. Quanti sono i polinomi primitivi di grado minore di 5 in $\mathbf{F}_2[X]$?
   d. E' vero che in $\mathbf{F}_7[X]$ due polinomi di grado $n$ si moltiplicano in $O(n^3)$ operazioni bit?

2 Dopo aver descritto e dimostrato l'algoritmo per determinare i coefficienti di Bezout di due interi, lo si applichi per calcolarli nel caso in cui i due interi sono 130 e 78.

3. Dopo aver definito il simbolo di Legendre dimostrare che il numero di elementi in $\mathbf{F}_p^*$ che hanno simbolo di Legendre pari a 1 è $(p - 1)/2$.
4. Spiegare in tutti i dettagli il funzionamento del crittosistema RSA e in particolare spiegare le accortezze necessarie per scegliere le chiavi.

5. Dato un intero dispari e composto $m$ si dimostri che l'insieme delle basi euleriane in $U(\mathbf{Z}/m\mathbf{Z})$ è un sottogruppo mentre quello delle basi forti non lo è.
6. Spiegare il funzionamento del crittosistema Massey–Omura e lo si illustri mediante un esempio esplicito.
7. Enunciare e dimostrare il teorema di classificazione dei sottocampi di $\mathbf{F}_{p^m}$.
8. Supponiamo $\mathbf{F}_8 = \mathbf{F}_2[\xi], \xi^3 = 1 + \xi$. Determinare il numero di punti di $E(\mathbf{F}_8)$ dove
$$E : y^2 + \xi y = x^3 + \xi$$
9. Supponiamo che $E$ sia un curva ellittica definita su $\mathbf{F}_{25}$, che $P \in E(\mathbf{F}_{25})$ sia un punto di ordine 7 e che $E$ abbia almeno due punti di ordine 2. Calcolare $\#E(\mathbf{F}_{25})$.

## APPELLO C — Roma, 7 Gennaio, 2013.

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:
   a. Determinate due fattori propri di 10000000000000000000400000000000000000003?
   b. È vero che $X^{97} - X + 3$ non ha radici monulo 97?
   c. Quanti sono i polinomi primitivi di grado 7 su $\mathbf{F}_7$?
   d. Perchè, se $M = p \cdot q$ è un modulo RSA, l'esponente di cifratura $e$ deve essere scelto in modo tale che $\gcd(e, \varphi(M)) = 1$?
2. Descrivere due algoritmi per il calcolo del massimo comun divisore di interi, determinarne la complessità e sfruttarli per calcolare con entrambi $\mathrm{MCD}(36, 63)$.
3. Determinare una stima per il numero di operazioni bit necessarie a moltiplicare due matrici $n^2 \times n^2$ i cui coefficienti sono minori di $2^n$.
4. Calcolare il seguente simbolo di Jacobi senza fattorizzare $\left(\frac{325893}{983832}\right)$.
5. Si illustri il funzionamento del metodo di fattorizzazione $\rho$ di Pollard.
6. Dopo aver descritto il crittosistema ElGamal su $\mathbf{F}_p$, se ne illustri il funzionamento con un esempio con $p = 29$.
7. Realizzare il campo $\mathbf{F}_{25}$ e determinare l'ordine di tutti i suoi elementi.
8. Data una curva ellittica $E$, definita su $\mathbf{F}_p$, si spieghi il metodo per calcolare l'ordine del gruppo $E(\mathbf{F}_{p^{100}})$.
9. Dopo aver dimostrato che è una curva ellittica su $\mathbf{F}_7$, calcolare la struttura del gruppo dei punti razionali di $y^2 = x^3 + x + 1$.

## APPELLO X — Roma, 14 Settembre 2012.

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:
   a. E' vero che se $E$ è una curva ellittica definita su $\mathbf{F}_{3^n}$, allora non ha mai un equazione della forma $y^2 = x^3 + ax + b$?
   b. E' vero che se tutti i fattori primi di $n - 1$ sono più piccoli di $\log n$, allora è possibile determinare un fattore non banale di $n$ in modo rapido? come?
   c. E' vero che se $p > 3$, il polinomio $X^2 + 1 \in \mathbf{F}_p$ non è mai primitivo ma qualche volta è irriducibile?
   d. E' vero che esistono modi per moltplicare interi con complessità inferiore a quella quadratica?

2 Se $n \in \mathbf{N}$, sia $\sigma(n)$ la somma dei divisori di $n$. Supponiamo che sia nota la fattorizzazione (unica) di $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Calcolare il numero di operazioni bit necessarie

per calcolare $\sigma(n)$. (*Suggerimento: Usare il fatto che $\sigma$ è una funzione moltiplicativa e calcolare una formula per $\sigma(p^\alpha)$* ).

3. Siano $m, n$ interi tali che $m \equiv 3 \bmod 4$, che $m \equiv 2 \bmod n$ e che $n \equiv 1 \bmod 8$. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{(5m+n)^3}{m}\right)$.
4. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. Considerare la curva ellittica $E : y^2 = x^3 - x$. Illustrare l'algoritmo appena descritto calcolando $[5](1,0)$ dove $(1,0) \in E(\mathbf{F}_{13})$.
5. Si dia la definizione di pseudo primo forte in base 2 e si mostri che se $n = 2^\alpha + 1$ è pseudo primo forte in base 2, allora $2^{2^\beta} \equiv -1 \bmod n$ per qualche $\beta < \alpha$.
6. Fissare una radice primitiva di $\mathbf{F}_{3^3}$ ed utilizzarla per simulare un scambio chiavi alla Diffie–Hellmann.
7. Dopo aver definito la nozione di polinomio primitivo su un campo finito, si calcoli la probabilità che un polinomio irriducibile $f$ di grado 8 su $\mathbf{F}_7$ risulti primitivo?.
8. Fattorizzare $f(x) = (x^{12} + 3x^4 + 1)(x^2 + x + 2)(x^{10} + x^2 + 1)$ su $\mathbf{F}_2$ e determinare il numero di elementi del campo di spezzamento di $f$.
9. Dopo aver verificato che si tratta di una curva ellittica, determinare (giustificando la risposta) l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_7$
$$y^2 = x^3 - x + 5.$$
.