CR410 (Crittografia a chiave pubblica)

AA13/14 – Compiti d'esame

- Risolvere il massimo numero di esercizi fornendo spiegazioni chiare e sintetiche.
- NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.
- 1 Esercizio = 4 punti.
- Tempo previsto: 2 ore.
- Nessuna domanda durante le prima ora e durante gli ultimi 20 minuti.

ESAME DI METÀ SEMESTRE — 4 Aprile 2014

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:
   (a) Esistono campi finiti con 48 elementi?
   (b) E' vero che non esistono identità di Bezout con coefficienti a segno discorde?
   (c) Fornire un esempio di campi finiti diversi con 16 elementi.
   (d) Scrivere tutti i polinomi primitivi in $\mathbf{F}_2[x]$ di grado minore uguale a 4.
2. Enunciare e dimostrare il Teorema di struttura dei sottocampi di $\mathbf{F}_{p^n}$. Lo si utilizzi per costruire un esempio di campo finito con esattamente 6 sottocampi.
3. Determinare tutti le radici primitive di $\mathbf{F}_5[\tau], \tau^2 = 2$.
4. Spiegare il funzionamento di alcuni sistemi crittografici che basano la propria sicurezza sul problema del logaritmo discreto.
5. Spiegare in dettaglio if funzionamento dell'Algoritmo Pohlig–Hellman.
6. Si applichi l'algoritmo delle approssimazioni successive per calcolare la parte intera del numero binario $\sqrt{101011101}$
7. Si determini il grado del campo di spezzamento su $\mathbf{F}_3$ del sequente polinomio $(x^{3^{11}} + 6x - x^9 + 30)(x^6 + 1)(x^9 + 15x - 1)$
8. Calcolare il massimo comun divisore $\gcd(273, 130)$ utilizzando sia l'algoritmo binario che quello esteso di Euclide. Utilizzare l'algoritmo di Euclide anche per calcolare un identità di Bezout.

ESAME DI FINE SEMESTRE — 26 Maggio 2014

1. Rispondere alle seguenti domande con una giustificazione di 1 riga:
   (a) E' possibile calcolare i simboli di Jacobi senza fattorizzare?

(b) I simboli di Jacobi hanno applicazioni in crittografia?

(c) E' possibile implementare RSA con un esponente di cifratura pari? perchè?

(d) Dare un esempio di curva ellittica $E/\mathbf{F}_p$ in cui $\#E(\mathbf{F}_p)$ è dispari.

2. Spiegare il funzionamento del crittosistema RSA.

3. Definire la nozione di pseudo primo di Miller Rabin e dimostrare che 91 è pseudo primo di Miller Rabin in base 10 e in base 22.

4. Calcolare il simbolo di Jacobi $\left(\frac{m}{n}\right)$ sapendo che $n \equiv 7 \bmod 4m$ e che $m \equiv 3 \bmod 28$.

5. Dopo aver definito la nozione di numero di Carmichael, si enunci e dimostri il criterio di Korselt.

6. Sia $E : y^2 = x^3 + Ax + B$ una curva ellittica su un campo $\mathbf{F}_p$ di caratteristica maggiore di 3. Dimostrare che se $P = (\alpha, \beta) \in E(\mathbf{F}_p)$ è un punto di ordine tre, allora α è una radice del polinomio:
$$\Psi_3(X) = 3X^4 + 6AX^2 + 12BX - A^2$$

7. Sapendo che una curva ellittica E su $\mathbf{F}_{101}$ ha un punto di ordine 50, cosa possiamo dire su $\#E(\mathbf{F}_{101})$?

8. Si determini $\#E(\mathbf{F}_{5^{20}})$ quando $E : y^2 = x^3 + 2x - 3$.

9. Si dimostri la legge di reciprocità quadratica.

APPELLO A 3 GIUGNO 2014

1. Si descriva un algoritmo per calcolare in tempo polinomiale la parte intera di $m^{1/2}$ per ogni intero positivo m.

2. Supponiamo che $e = 5$ sia la chiave di cifratura di un crittosistema RSA con modulo $n = 53 \cdot 43$. Si calcoli la chiave d di decifratura.

3. Dimostrare che in $\mathbf{F}_p$ l'equazione $x^m \equiv 1 \bmod p$ ammette $\gcd(p-1, m)$ soluzioni. Quante ne ammette in $\mathbf{Z}/(101 \cdot 103)\mathbf{Z}$?

4. Definire il simbolo di Jacobi ed illustrare un algoritmo polinomiale per calcolarlo.

5. Spiegare il funzionamento dei protocolli crittografici incontrati nel corso.

6. Si determini la probabilità che un polinomio irriducibile su $\mathbf{F}_2$ di grado 8 risulti primitivo.

7. Determinare tutti i generatori di $\mathbf{F}_5[\tau], \tau^2 = 2$ e di ciascuno determinare il polinomio minimo.

8. Determinare la struttura del gruppo dei punti razionali di una curva ellittica definita su $\mathbf{F}_{101}$ sapendo che ha un punto P di ordine 41.

9. Siano $E_1 : y^2 = x^3 + x + 1$ e $E_2 : y^2 = x^3 + x + 4$ due curve definite su $\mathbf{F}_5$. Dopo aver verificato se sono ellittiche determinarne ka struttura della gruppo dei punti razionali su $\mathbf{F}_5$ e si $\mathbf{F}_{5^2}$.

APPELLO B 30 GIUGNO 2014

1. Si descriva un algoritmo per calcolare in tempo polinomiale la parte intera di $m^{1/2}$ per ogni intero positivo m.

2. Supponiamo che $e = 5$ sia la chiave di cifratura di un crittosistema RSA con modulo $n = 53 \cdot 43$. Si calcoli la chiave d di decifratura.

3. Dimostrare che in $\mathbf{F}_p$ l'equazione $x^m \equiv 1 \bmod p$ ammette $\gcd(p-1, m)$ soluzioni. Quante ne ammette in $\mathbf{Z}/(101 \cdot 103)\mathbf{Z}$?

4. Definire il simbolo di Jacobi ed illustrare un algoritmo polinomiale per calcolarlo.

5. Spiegare il funzionamento dei protocolli crittografici incontrati nel corso.

6. Si determini la probabilità che un polinomio irriducibile su $\mathbf{F}_2$ di grado 8 risulti primitivo.

7. Determinare tutti i generatori di $\mathbf{F}_5[\tau], \tau^2 = 2$ e di ciascuno determinare il polinomio minimo.

8. Determinare la struttura del gruppo dei punti razionali di una curva ellittica definita su $\mathbf{F}_{101}$ sapendo che ha un punto P di ordine 41.

9. Siano $E_1 : y^2 = x^3 + x + 1$ e $E_2 : y^2 = x^3 + x + 4$ due curve definite su $\mathbf{F}_5$. Dopo aver verificato se sono ellittiche determinarne ka struttura della gruppo dei punti razionali su $\mathbf{F}_5$ e si $\mathbf{F}_{5^2}$.

APPELLO C — Roma, 30 GENNAIO 2015

Si descrivano:

1. L'algoritmo di Euclide (per l'identità di Bezout) e suo il tempo di esecuzione. ;

2. Gli algoritmi per la moltiplicazione degli interi a la loro complessità;

3. L'algoritmo Baby Steps Giant Steps per il calcolo dell'ordine di una curva ellittica su un campo finito;

4. L'algorimo di Pholig–Hellman per il calcolo dei logaritmi discreti;

5. La varie definizioni di pseudo primi e le loro principali proprietà.

6. Determinare ordine e struttura di $E(\mathbf{F}_7)$ dove $E : y^2 = x^3 - 1$.

7. Dopo aver descritto quali sono i fattori irriducibili in $\mathbf{F}_1 1[x]$ di $x^{11^6} - x$ (p primo), si determini il numero di tali fattori che sono primitivi.

8. Dopo aver fornito la definizione di numero di Carmichael, si enuncino e dimostrino le principali proprietà dei numeri di Carmichael fornendone esempi.

9. Dimostrare che su $\mathbf{F}_q, q$ dispari, c'è sempre una curva ellittica con gruppo dei punti razionali non ciclico.

10. Si descrivano i principali algoritmi di cifratura e decifratura.

APPELLO X — Roma, 3 SETTEMBRE 2014

Si descrivano:

1. L'algoritmo dei quadrati successivi;

2. L'algoritmo per calcolare i simboli di Jacobi (senza fattorizzare);

3. L'algoritmo Baby Steps Giant Steps per il calcolo dei logaritmi discreti;

4. L'algorimo di Pholig–Hellman per il calcolo dei logaritmi discreti;

5. Dopo aver descritto la nozione di algoritmo probabilistico di tipo Montecarlo, l'algoritmo di Miller–Rabin.

6. Determinare ordine e struttura di $E(\mathbf{F}_7)$ dove $E : y^2 = x^3 + 3$.

7. Dopo aver descritto quali sono i fattori irriducibili in $\mathbf{F}_p[x]$ di $x^{p^4} - x$ (p primo), nel caso in cui $p = 2$, li si elenchino tutti specificando quali tra questi sono primitivi.

8. Siano n e m interi tali che $m \equiv 3 \bmod 4$, $m \equiv 2 \bmod n$ e $n \equiv 1 \bmod 8$. Si calcoli il simbolo di Jacobi $\left(\frac{(5m+n)^7}{m}\right)$.

9. Dimostrare che se $\mathbf{F}_q$ è un campo finito di caratteristica dispari, allora esiste sempre una curva ellittica su $\mathbf{F}_q$ con gruppo dei punti razionali non ciclico.

10. Si descrivano i principali algoritmi di cifratura e decifratura.