Middle East Technical University

Institute of Applied Mathematics

Cryptography Program

Ph.D. Qualifying Exam

May 2021

There are a total of 8 questions: two questions from group A and three questions from each of groups B and C. Please choose and answer 5 of the given 8 questions by discarding one question from each group.

May 21, 2020

Time allowed is 3 hours

IAM 503 APPLICATIONS OF FINITE FIELDS

A.1. Let $q = 2^m$ be power of 2 and $\mathbb{F}$ be a finite field of q elements.
(a) Is it possible to choose $z \in \mathbb{F}_q \backslash \{1\}$ such that the equation

$$x^2 + x + \frac{1}{1+z^2} = 0$$

has no solution $x \in \mathbb{F}_q$. If so, choose one such z for m is even and m is odd. If not, prove that not possible.

(b) Is it possible to choose $z \in \mathbb{F}_q \backslash \{1\}$ such that the equation

$$x^2 + x + 1 + z^2 = 0$$

has no solution $x \in \mathbb{F}_q$. If so, choose one such z for m is even and m is odd. If not, prove that not possible.
Hint: Consider the cases m is even and odd separately.

A.2. Let $f(x) = x^5 + x^4 + 1 \in \mathbb{F}_2[x]$.
(a) Find the splitting field E of f over $\mathbb{F}_2$.
(b) Find all subfields of E.
(c) Find the number of elements in E, which is not contained in any proper subfield.
(d) Find the conjugates of $\alpha \in E$ with respect to the all subfields of E.

IAM 502 STREAM CIPHERS
IAM 512 BLOCK CIPHERS

B.1.

a) Let $E_K(P)$ be the encryption function of a Feistel network cipher which uses the function $f(k, m)$ where k is the round sub-key and m is the right half of the round input. Suppose that $f(x, \bar{y}) = f(\bar{x}, y)$ where $\bar{a}$ means the bitwise complement of the binary string a. Show that $E_{\bar{K}}(\bar{M}) = \overline{E_K(M)}$.

b) Explain why a Feistel structure based block cipher must have at least three rounds.

B.2.

a) For $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ what is the nonlinearity of f? Can we find f with largest nonlinearity for an arbitrary large even integer n? What about for odd integer n? Namely, is it known what the largest nonlinearity and examples of functions satisfying the nonlinearity?

b) What is the LAT of f? Explain how that the distance of f to the affine linear function $x \to a \cdot x + b$ is related to the values of LAT table of f at the entry (a, b).

B.3. Consider the binary sequence: 0,1,0,1,1,1,0,0,1,1,.
Using Berlekamp Massey Algorithm, either determine the LFSR (that is, connection polynomial) of length 5 that produces this sequence or prove that no LFSR of length 5 can produce this sequence.

IAM 504 PUBLIC KEY CRYPTOGRAPHY
IAM 505 ELLIPTIC CURVES IN CRYPTOGRAPHY

C.1.
a) Explain the RSA encryption system (key generation, encryption, and decryption) and prove that the decryption works correctly.

b) Is it secure to use the public exponent $e = 3$ in the textbook RSA? Prove your answer.

c) Let n be the product of two primes. Prove that the problem of factoring n is equivalent to the problem of finding $\phi(n)$, Euler's phi function.

C.2. a) What is a malleable encryption?

b) Explain the ElGamal encyption system (key generation, encryption, and decryption) and prove that the decryption works correctly.

c) Is EGamal system malleable? Prove your answer.

d) Explain the Pohlig-Hellman algorithm for solving the discrete logarithm problem? How should the parameters be selected in order to avoid this attack?

C.3. It is known that there are two classes of elliptic curves over the finite field $\mathbb{F}_{3^n}$:

(i) $y^2 = x^3 + ax^2 + b$, $\Delta = -a^3b \neq 0$
(ii) $y^2 = x^3 + ax + b$, $\Delta = -a^3 \neq 0$

a) Write the weighted projective equations for $w = (c, d, 1)$, $\gcd(c, d) = 1$ associated to these 2 classes when $c = 2, d = 3$ (Jacobian Coordinates) and $c = 1, d = 2$ (LD Coordinates).

b) Find the identity element of the given classes elliptic curves for both cases of Jacobian and LD coordinates.

c) Find the formulas of $-P$ on two elliptic curves for both Jacobian and LD coordinates.

d) Explain shortly the importance of the usage of different weighted projective coordinates in Elliptic Curve Cryptography.