**Middle East Technical University**

**Institute of Applied Mathematics**

**Cryptography Program**

# Ph.D. Qualifying Exam

**November 2020**

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.

November 27, 2020

Time allowed is 3 hours

## IAM 503 APPLICATIONS OF FINITE FIELDS

**A.1.** Let $\mathbb{F}$ be a finite field of $q$ elements and the characteristic of $\mathbb{F}$ be $p$. Prove that for every element of $\mathbb{F}$ there exists exactly one $p$-th root of it. That is, prove that $\forall x \in \mathbb{F}, \exists! a \in \mathbb{F}$ with $a^p = x$.

**A.2.** Find the 15th cyclotomic polynomial $Q_{15}(x)$
i) over $\mathbb{F}_2$.
ii) over $\mathbb{F}_3$.

# IAM 502 STREAM CIPHERS
# IAM 512 BLOCK CIPHERS

**B.1.** Define briefly the concept "propagation characteristic of order $k$" for a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Obtaining the related formulas, explain how this characteristic is measured using the Walsh transform.

**B.2.** Explain the principles of shrinking generator and self shrinking generator. Show that a self shrinking generator can be regarded as a shrinking generator and vice versa. Obtain an upper bound for the period and linear complexity of a shrinking generator in terms of the lengths of m-LFSRs used for the generator.

**B.3.** Let the probability of $\alpha \to \beta$ be the probability that for a pair with the input difference $\alpha$, the output difference is $\beta$, among all the possible pairs.

**a)** Can $\alpha \to 0$ be nonzero, for a nonzero value of $\alpha$?

**b)** Consider the following $S$-Box:

| $X$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| $S[X]$ | 001 | 101 | 110 | 000 | 111 | 011 | 010 | 100 |

Determine 010 → 111.

**c)** Consider an $S$-box from $F_2^n$ to $F_2^m$. What is the sum of the entries in each column of the difference distribution table. Show your answer.

## IAM 504 PUBLIC KEY CRYPTOGRAPHY
## IAM 505 ELLIPTIC CURVES IN CRYPTOGRAPHY

**C.1.** a) Describe RSA cryptosystem (explain the key generation, encyption and decryption algorithm).
b) Prove that RSA decryption works correctly.
c) What are the attacks to RSA? Discuss the ways of avoiding those atacks?

**C.2.** a) Explain the index calculus algorithm for computing discrete logarithms.
b) Given $\mathbb{Z}_{29}^* =< 2 >$. Find $x$ satisying $2^x \equiv 11$ in $\mathbb{Z}_{29}^*$ using index calculus method with the relations $2^2 \equiv 4 \mod 29$, $2^7 \equiv 12 \mod 29$, and $2^{22} \equiv 5 \mod 29$.
c) Discuss the use of the index calculus algorithm for elliptic curves.

**C.3.** Let $E : y^2 = x^3 + ax + b$ be a curve over $\mathbb{F}_p$ for a prime number $p > 3$.
**a)** Show that $E$ is non-singular if $4a^3 - 27b^2 \neq 0$.
**b)** Find the formula of point addition of two affine points $(x_1, y_1)$ and $(x_2, y_2)$ on $E$.
**c)** Find the formula of point doubling of an affine point $(x_0, y_0)$ on $E$.
**d)** Find all the points on the elliptic curve defined by $y^2 = x^3 + 7x + 6/\mathbb{F}13$.
**e)** Prove that $E(\mathbb{F}_{13})$ is a cyclic group. Find a generator $G$ in this group.
**f)** Choose your private key $d = 3$ and find your corresponding public key on $E(\mathbb{F}_{13})$ for the domain parameter $G$. (Use the formulas obtained in b,c)
**g)** Write the signature generation and verification steps in ECDSA.
**h)** If a signer uses the same random number for two distinct messages, show that an attacker can find his private key.