CHAPTER 3
CRYPTOGRAPHY AND TECHNICAL FOUNDATIONS

From : Mastering Blockchain

By – Imran Bashir

www.packet.com

Introduction

Cryptography is

- The science of making information secure in the presence of adversaries.
- It provides a means of secure communication in the presence of adversaries.

Cryptography provides

- **Confidentiality, Integrity, Authentication**, (Entity Authentication and Data origin authentication) and **nonrepudiation.**

Mathematics in Cryptography

- **Set -** A set is a collection of distinct objects, for example, $X= \{1, 2, 3, 4, 5\}$.
- **Group -** A group is a commutative set with one operation that combines two elements of the set.
  - Let G be a non-empty set and let $\star$ be a binary operation on G:
  - (bop) $\star$: $G \times G \to G$, (a, b) 7$\to$ $a \star b$.
  - Then $(G; \star)$ is a group if the following axioms are satisfied:
  - (G1) associativity: $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in G$
  - G2) identity element: there exists $e \in G$ such that $a \star e = e \star a = a$ for all $a \in G$.
  - (G3) inverses: for any $a \in G$ there exists $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.
  - If in addition the following holds
  - (G4) commutative: $a \star b = b \star a$ for all $a, b \in G$ then $(G; \star)$ is called an **Abelian Group**, or simply a commutative group.

Mathematics in Cryptography

- **Field -** A field is a set that contains both additive and multiplicative groups.
  - More precisely, all elements in the set form an additive and multiplicative group.
  - It satisfies specific axioms for addition and multiplication.
  - For all group operations, the distributive law is also applied.
  - The law dictates that the same sum or product will be produced even if any terms or factors are reordered.
- **A finite field -** A finite field is a field with a finite set of elements. Also known as Galois fields.
  - These structures are of particular importance in cryptography as they can be used to produce accurate and error-free results of arithmetic operations. For example, prime finite fields are used in elliptic curve cryptography to construct discrete logarithm problem.

Mathematics in Cryptography

- **Order -** This is the number of elements in a field. It is also known as the cardinality of the field.
- **Prime fields -** This is a finite field with a prime number of elements.
  - It has specific rules for addition and multiplication,
  - Each nonzero element in the field has an inverse.
  - Addition and multiplication operations are performed modulo p.
- A cyclic group - A cyclic group is a type of group that can be generated by a single element called the group generator.
  - In other words, if the group operation is repeatedly applied to a particular element in the group, then all elements in the group can be generated.

Mathematics in Cryptography

- **Ring** - If more than one operation can be defined over an abelian group, that group becomes a ring.
  - A ring must have closure
  - Associative and distributive properties.
- More on algebraic structures

Entity authentication

- Entity authentication is the assurance that an entity is currently involved and active in a communication session.
- Traditionally, users are issued a username and password, which are used to gain access to the platforms they are using.
- This is called single factor authentication as there is only one factor, namely something you know, that is, the password and username
- For more security now a days we use more factors for authentication

Data origin authentication

- Also known as *message authentication*, this is an assurance that the source of information is verified.
- It implies data integrity because if a source is confirmed, then data must not have been altered.
- Various methods, such as Message Authentication Codes (MACs) and digital signatures are most commonly used.

Non-repudiation

- Non-repudiation is the assurance that an entity cannot deny a previous commitment or action by providing unforgeable evidence.
- It is a security service that provides unforgeable evidence that a particular action has occurred.
- This property is very necessary in disputable situations whereby an entity has denied actions performed, for example, placing an order on an e-commerce system.
- The non-repudiation protocol usually runs in a communication network.

Cryptographic primitives

This image cannot currently be displayed.

A model showing the generic encryption and decryption model

Elliptic curves

- Elliptic curve is an algebraic cubic curve over a field, which can be defined by an equation shown here.

$$y^2=x^3+ax+b$$

- The curve is non-singular, which means that it has no cusps or self-intersections.
- It has two variables *a, b,* along with a point of infinity.
- Here, *a, b* are integers that can have various values and are elements of the field on which the elliptic curve is defined.
- Elliptic curves can be defined over reals, rational numbers,
- complex numbers, or finite fields.
- For cryptographic purposes, elliptic curve over prime finite fields is used instead of real numbers.
- Different curves can be generated by varying the value of *a, b.*

Elliptic Curve Applications

- Mostly prominently used cryptosystems based on elliptic curves are **Elliptic Curve Digital Signatures Algorithm** (ECDSA)
- **Elliptic Curve Diffie-Hellman** (**ECDH**) key exchange
- More on ECC : https://youtu.be/2RVLBUncHJk