08/02/23

DATE : / /
PAGE NO. : 1

Mathematical Foundation for Blockchain
Assignments 1.

Q1 What is cryptography? Differentiate between classical cryptography and modern cryptography.

A (I) Cryptography is technique of securing information and communications through use of codes so that only the authorized personnel can understand and process it.

(II) In Cryptography, the techniques which are used for protection are obtained from mathematical concepts and a set of rules based calculations known as algorithms to convert messages in ways that are hard to decode

(III) The algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions.

(IV) Advantages

(i) Access Control
Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource.

(ii) Secure Communication
For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the internet.

(iii) Protection against attacks
Cryptography aids in defence against various kinds of assaults, including replay and man-in-the-middle attack. It provides strategies for spotting and stopping these attacks

PAGE NO. :

Classical Cryptography	Modern Cryptography
(I) It manipulates traditional characters i.e. letters and digits directly.	(I) It operates on binary bit sequences.
(II) It is mainly based on 'security through obscurity'. The techniques employed for coding were secret and only the people involved in communication knew about them	(II) It relies on publicly known algorithms for coding. Secrecy is obtained through a key which is used as the seed for the algorithm.
(III) It requires the entire cryptosystem for communicating confidentiality.	(III) Modern cryptography requires parties intrusted in secure communication to possess the secret key only

Q2 What are the various cryptography primitives. Explain the role of these primitives in cryptography.

A (I) Cryptographic primitives are the basic building blocks of a security protocol or system. You will learn about cryptographic algorithms.

(II) These algorithms are crucial for creating safe protocols and systems. A security protocol is a series of actions made to use the proper security mechanisms in order to accomplish the necessary security goals.

(III) These are the low level algorithms that are used to build algorithms. The programmers develop new cryptographic algorithms with the help of cryptographic primitives.

(IV) Role of primitives :

(1) Security

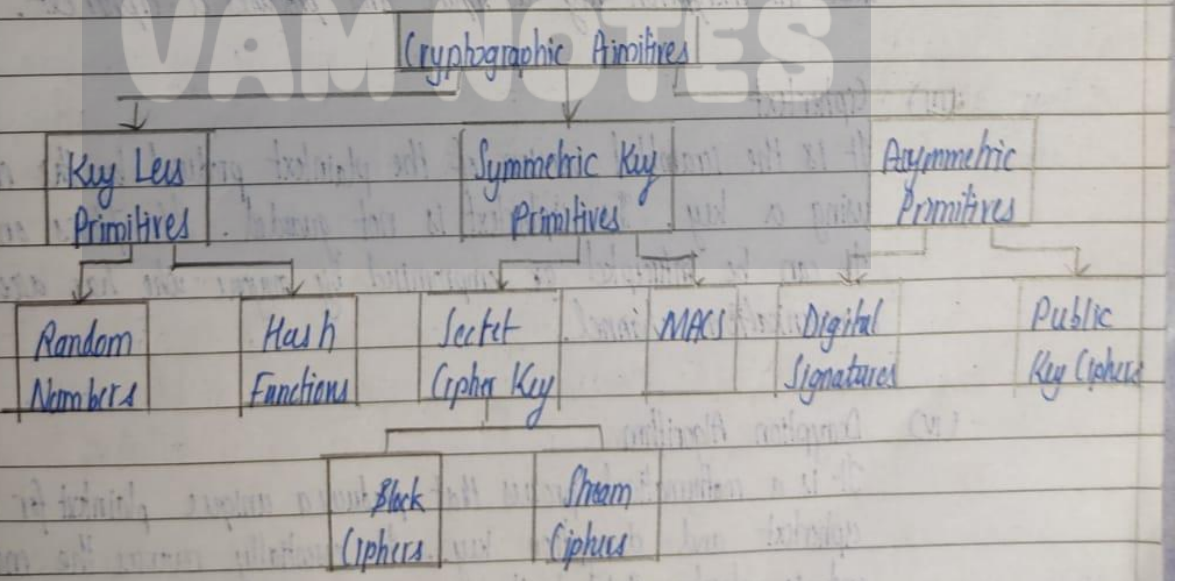
DATE : / /
PAGE NO. : 3

To secure a transaction in the network or confidential information, strong cryptography is required. So cryptographic primitives are used to develop high-level algorithms.

(ii) Encryption and Decryption
The cryptographic primitives are used to develop encryption and decryption algorithms. Encryption and decryption is done whenever required.

(iii) Validation
The validation of data is done with the help of digital signatures. These digital signatures are public key primitives which the receivers use to validate the message.

(iv) Specific
Cryptographic primitives are very specific in nature. It means one cryptographic primitive can perform only one function.



The taxonomy of cryptographic primitives

Q3 Explain the various components of a basic cryptosystem.

A (I) A cryptosystem is an implementation of cryptographic techniques and their accompanying techniques and infrastructure to provide information security services.

(II) A cryptosystem is also referred to as a cipher system.

(III) Cryptosystems are used for sending messages in a secure manner over the Internet, such as credit card information and other private data.

(IV) Components of a Cryptosystem:

(i) Plaintext
It is the data to be protected during transmission.

(ii) Encryption Algorithm
It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithms that takes plaintext and an encryption key as input and produces a ciphertext.

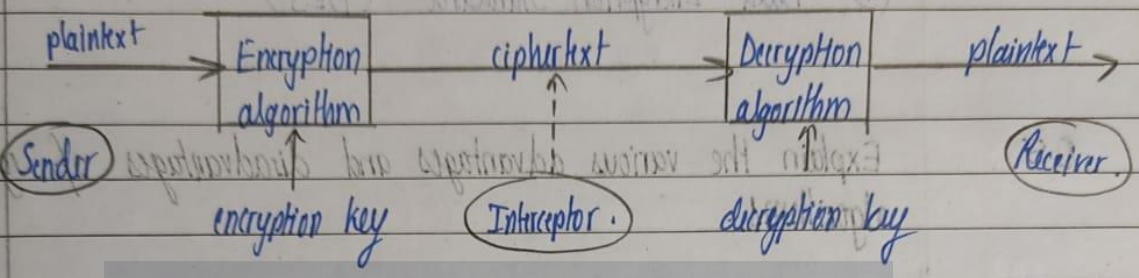
(iii) Ciphertext
It is the scrambled version of the plaintext produced by the encryption algorithm using a key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

(iv) Decryption Algorithm
It is a mathematical process that produces a unique plaintext for any given ciphertext and decryption key. It essentially reverses the encryption algorithm and is closely related to it.

(v) Encryption Key
The value known to the sender that is used to compute the ciphertext for given

plaintxt.

(vi) Decryption Key
The value known to the receiver that is used to decode the given ciphertxt into plaintxt.



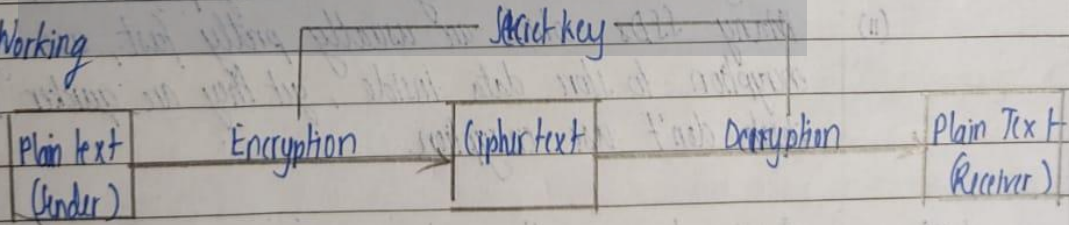
Q4 What is symmetric key cryptography? Explain the working of symmetric key cryptography with suitable diagram.

A (I) Symmetric key cryptography is a type of encryption where a similar keys are used to both encrypt and decrypt messages.

(II) It is also known as shared-key, secret key, single key, one key and sometimes private key cryptography.

(III) Both the sender and receiver use common keys to encrypt and decrypt the message. The secret key is known only to the sender and to the receiver.

(IV) Working



(i) Before starting the communication, sender and receiver share the secret key.
(ii) The secret key is shared through some external means.
(iii) At sender side, sender encrypts the message using his copy of the key.
(iv) The cipher text is then sent to the receiver over the communication channel.

(v) At receiver side, receiver decrypts the cipher text using his copy of key.
(vi) After decryption, the message converts back to readable format.
(vii) Some encryption algorithms used are :
(i) Advanced Encryption Standard (AES)
(ii) Data Encryption Standard (DES)

Q5 Explain the various advantages and disadvantages of symmetric key algorithms.

A (I) Advantages of symmetric key algorithms.

(I) Exceptionally safe :
(i) Symmetric key encryption can be highly secure when it employs a secure algorithm. AES is one of the most extensively used symmetric key encryption schemes.
(ii) Using ten desktop machines, brute-force guessing the key using its most secure 256 bit length would take a billion years.

(II) Speed
(i) It is pretty simple to encrypt and decrypt symmetric key data resulting in excellent reading and writing performance.
(ii) Many SSDs, which are usually pretty fast, use symmetric key encryption to store data inside, yet they are quicker than hard drives which don't use encryption.

(III) Requires low computer resources
(i) When compared to public key encryption, single key encryption uses fewer computer resources.

(IV) Minimizes message compromises.
A distinct secret key is utilized for communication with each party,

preventing a widespread message security breach.

(II) Only the messages sent by a specific pair of sender and receiver are affected if a key is compromised. Other people's communications are still safe.

Disadvantages of symmetric algorithms

(I) No guarantee of authenticity

(1) Because both the sender and receiver have the same key, messages cannot be validated as coming from a specific user.

(II) Key Sharing

(1) The most significant drawback of this is that the key must be communicated to the party with which you share data.

(II) There needs to be a secure method of delivering the key to the other party.

(III) Compromised Security can cause More Damage

(1) When two way communications are encrypted by symmetric encryption, both sides of the conversations are vulnerable.

(II) Someone who obtains your private key can decode communications sent to you, but they won't decipher messages sent to the other person as they are encrypted with a different key pair.

Q6 Why is assymmetric key cryptography called public key cryptography?

A (I) The most significant advantage of using assymmetric key cryptography over symmetric encryption is the non-reliance on a single point of failure key.

(II) Since the key used to encrypt is already public, the key used to decrypt the data is supposed to be private and must not be shared.

(III) Therefore, assymmetric key cryptography is also called public key cryptography because of its open nature.

(IV) This contrasts with symmetric encryption, where the single key used for both encryption and decryption is supposed to be kept secret.

Q7 What is asymmetric key cryptography? Explain the working of asymmetric key cryptography with suitable example.

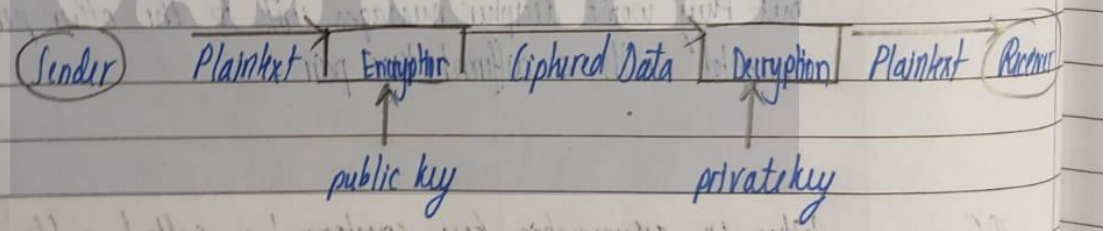
A (I) Asymmetric encryption, also known as private key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data.

(II) The pair of keys include a public key, which can be shared with anyone and a private key which is kept secret by the owner.

(III) Asymmetric cryptography is scalable for use in high and ever expanding environments where data are generally exchanged between different communication partners.

(IV) Asymmetric cryptography is used to exchange the secret key to prepare for using symmetric cryptography to encryption information.

(V) Working:



(i) All the data is sent through plaintxt. It is then encrypted with a ~~private~~ public key. The ciphered data uses a private key to decrypt.

(ii) It promotes secure key exchange which is a critical feature in secure communication.

(VI) Examples:

(i) Rivest Shamir Adleman (RSA)

(ii) Digital Standard Signature (DSS)
(iii) Elliptical Curve Cryptography (ECC)
(iv) Diffie Hellman exchange method
(v) TLS / SSL protocol

TLS / SSL

(i) It is a protocol for encrypting communications over a network. TLS uses both asymmetric and symmetric encryption.
(ii) During a TLS handshake, the client and server agree upon two keys to use, called 'session keys'.
(iii) The TLS handshake itself makes use of asymmetric cryptography for security while the two sides generate symmetric session keys, and in order to authenticate the identity of the website's origin server.

Q8 What is elliptical curve cryptography? Explain the working of elliptical curve cryptography with suitable diagram

A :

(I) ECC is an asymmetric encryption algorithm that employs the algebraic architecture of elliptical curves with finite fields.

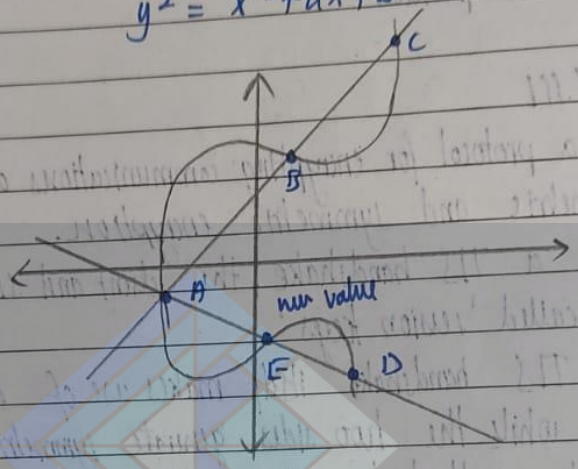
(II) ECC is comparable to RSA. While RSA's security is dependent on huge prime numbers, ECC leverages the mathematical theory of elliptic curves to achieve the same level of security and considerably smaller keys.

(III) Working

(i) An elliptic curve is a curved line that loops around and mirrors up with two axes at the end of its journey. Along the x axis of the graph, the curve is completely symmetrical in every direction.
(ii) It employs a public key cryptography. Keys are not obtained by the more conventional approach of creating them as the product of big prime numbers, but rather by taking use of the features of an elliptic curve equation

(iv) The nodes and edges of the graph may be represented mathematically using the following equation:

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



(v) ECC is neither fundamentally better nor less secure than other options like RSA. The built in efficiency that ECC gives while encrypting and decrypting data is the primary benefit that it offers.

For reference purposes only. Not liable for any misuse or misinterpretation.
We're interested in providing notes and assignments for free because college is more than just about submissions! :D
Thank you for all your support!

Our repo - https://github.com/VAMNotes/VAMNotes (please star and share)

Our telegram - https://t.me/+Qva7WM1UEdc2YzNl