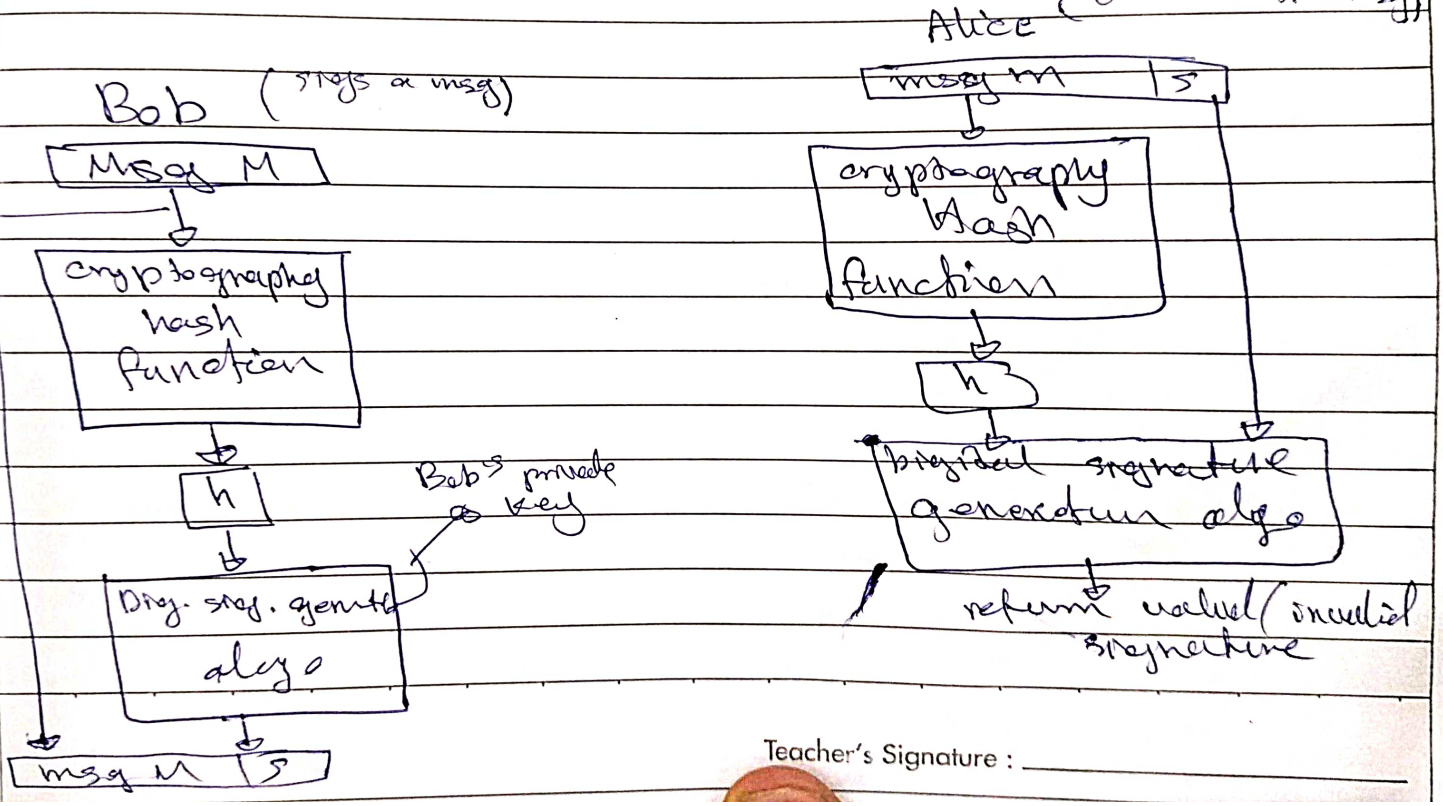
Tuesday 27th "no test IDIW

Unit 13:- Digital Signature :- imp. development in public-key cryptography provides set of security capabilities that's difficult to implement other ways.



Teacher's Signature : _____

Expt. No.---------- Page No.----------

unit 4 Advanced Encryption Standard (AES):-
was published by (NIST) in 2001. Is symmetric cipher block to replace DES as the approved standard for a wide range of application.
structure of AES is simpler than RSA. In AES all operation are done with 8 bit bytes.
Appendix B:- uses evaluation criteria used by NIST to select candidates for AES, adds rational for picking Rijndael (winning candidate). It includes any symmetric, Finite Field Arithmetic:- Finite It also does all operation (+, -, /, ×) in Finite field of GF(2^8). A field in which (+, -, ×, ÷) are done without leaving a set.
AES Structure:- key length can be 16, 24, 32 byte (128, 192, 256 bits) each block is copied into a state array, then get modified in each stage. (1st 4 bytes occupy first column, 2nd 4 bytes occupy 2nd column) then the key gets expand in 4×4 matrix. no. of rounds depend upon key length.
AES Transformation:- 4 trans formation
Key Expansion Algorithm:- takes as input a 4 word (16 byte) and produce a linear array of 44 words (176 bytes). AddRoundKey,
Page 191 Rationale:- Rijndael designed expansion key algo. to be resistance to known cryptanalytic attacks the specific criteria used → [DAEM99].

Unit 4:- A has function H accepts a variable-length block of data M as input and produce a fixed-size hash value h=H(M). a good hash produce good output.
- Hash needed for security app. is cryptographic hash function.
- hash functions often determine wether or not data has changed.
- Hash looks at range of app in which it is employed.

Msg Authentication:- is mechanism or service to verify integrity of msg. (sent & received securely) (Id of sender and R—r). (we can use hash function not having encryption in it)

Teacher's Signature : _____

6:45 Library...

Date 24/09/22

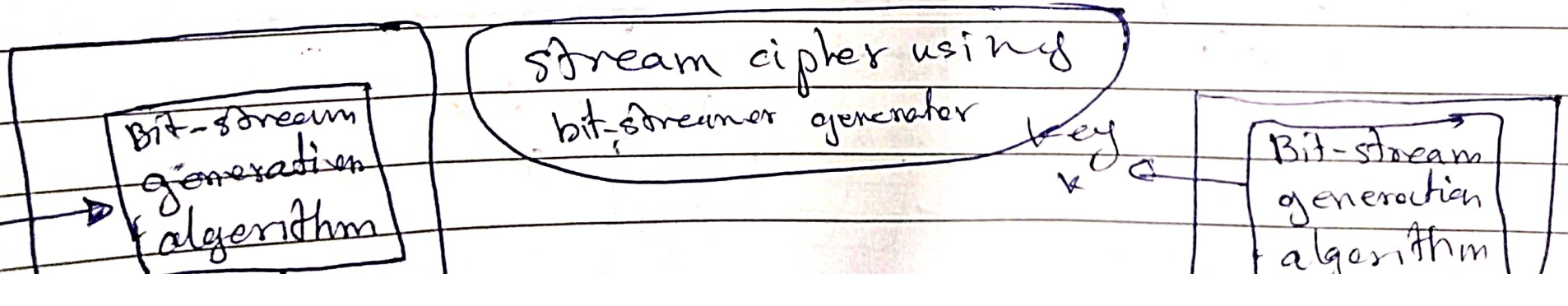
Expt. No.---------- Page No. DTU...

unit 4: ①

Traditional Block Cipher Structure:- imp. symmetric Cipher block encryption algo. in current use are based on a structure referred to Fiestel Block Ciphers [FEIS73], that is why its impt. to examine Feistel cipher by comparison.

Stream Cipher and Block Ciphers:-

- Stream cipher encrypts adjacent plain stream one bit/byte at a time. Exa: auto keyed & Vigenère ciphers and Vernam Cipher. If key is random then its breakable. key should be provided through secure channel.
- Block Cipher: blocks of plaintext is treated as a whole and used to produce ciphertext block of equal length.



6:45 Library...

Date 24/09/22

Expt. No.---------- Page No. DTU...

unit 4: ①

Traditional Block Cipher Structure:- imp. symmetric cipher block encryption algo. in current use are based on a structure referred to Feistel Block Cipher [FEIS73], that is why its impt. to examine Feistel cipher by comparison.

Stream Cipher and Block Ciphers:-

- Stream cipher encrypts digitized data stream one bit/byte at a time. Exa: auto keyed & Vigenère ciphers and Vernam Cipher. If key is random then its breakable. key should be provided through secure channel.
- Block Cipher: blocks of plaintext is treated as a whole and used to produce ciphertext block of equal length.

Unit 4 :-

② Reversible Mapping :- 2^n possible diff. plaintext block, for encryption to be reversible (decryption to be possible) each must produce unique ciphertext block.

Feistel Ciphers :- proposed [EEIS73] to approximate the ideal block cipher by utilizing the concept of a product ciphers, which is the execution of 2 or more simple ciphers. final result is cryptographically stronger than any of the component ciphers. key length = 128 bits, block length = n bits. 2^k possible transformations (k: Allacity) than $2^n!$ transformations.

Substitution: Each plaintext element is uniquely replaced by corresponding cipher elements.

Permutation: A sequence plain text elements is replaced by a permutation of that sequence.

Diffusion :- statistical structure of plaintext dissipate into long-range statistical ciphertext.

Confusion :- seeks to make relationship b/w statistics of ciphertext and value of encryption key as complex as possible to prevent attempts to discover the key.

Block size :- larger block size greater security, speed reduces in encryption-decryption (diffusion)

key size : larger key size greater security, speed reduces in " " (confusion).

No. of round : more rounds more security typically 16 rounds.

subkey gen. algo: Greater complexity in algo leads to greater difficulty of cryptanalysis.

- Two Considerations in Feistal ciphers: Feast software encry/decrypt. Ease analysis.
- (AES 2001, DES 1977). For DES, data are encrypted in 64-bit blocks using 56 bit key.

The Avalanche Effect :- Small change in plaintext or key should bring larger effect on ciphers. a change in 1 bit of plaintext or key produce many bit change called --effect.

Use of 56-bit keys: With a key length of 56 bits there are 2^{56} possible keys. (approximate)

Unit 5

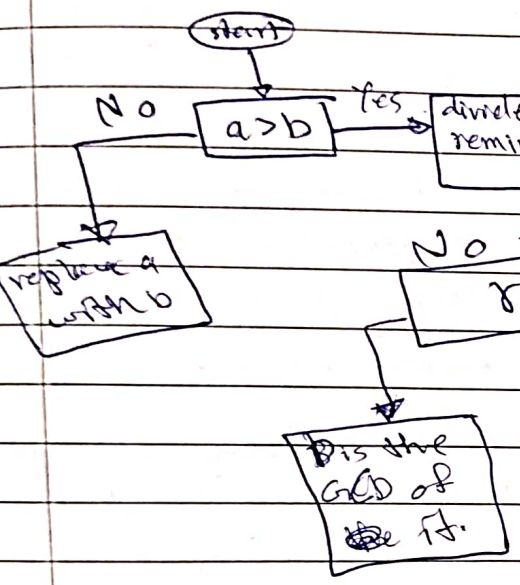
② Finite Field :- AES, Elliptic Curve rely on finite field. Examples ~~GCD~~ GCM, CMAC. are subset of fields, these fields with finite number of elements.

Field :- are subject of larger class algebraic structure called rings.

Groups, Rings, fields are elements of abstract algebra, in abstract Algebra is link with sets in which the elements can be operate algebrically.

Ordinary Polynomial Arithmetic: A polynomial of degree n (integer $n \geq 0$) is an expression of the form $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$.

2. Euclidean Algo:- Basic technique of number theory. it determine Greatest Common divisor of 2 pt integers.



GCD of 710, 310

$710 = 2 \times 310 + 90$

$310 = 3 \times 90 + 40$

$90 = 2 \times 40 + 10$

$40 = 4 \times 10$.

~~Molecular~~ ~~Modular Arithmetic~~

Miller - Rabin Algo:- It can be shown [KNUT98] given odd number (n) which is not integer a with $1 < a < n-1$. The probability that TEST will be shown inconclusive (fails to detect that n is an integer not a prime) is $1/4$.

Deterministic Primality Algo:- till 2002, No method to prove primality of very large number. in 2004, AKS developed simple deterministic algo that determined whether the large number is prime or not

Distribution of primes:- $0.5 \ln(n)$ $n = 2^{200} \Rightarrow 0.5 \ln(2^{200})$.

Chinese Remainder Theorem (CRT): useful number theory, it says it is possible to reconstruct integer in a certain range.

Binary Operator mod: If a & n is integer, we define a mod n to be the remainder when a is divided by n. The integer "n" is modulus, remainder is residue

Expt. No. ....

unit 1 Information Security Audit Exam Notes

Cryptography 4 types.

- → Symmetric encryption: hides contents of blocks data at any size from sms, file, key, pass..
- → Asymmetric encryption: hides small blocks of data like encryp" key, hash func", used in digital sign
- → Data integrity algorithm: protects block of data like messages from alternation
- → Authentication protocols: authenticates identity of entities based on use of crypto-Alg

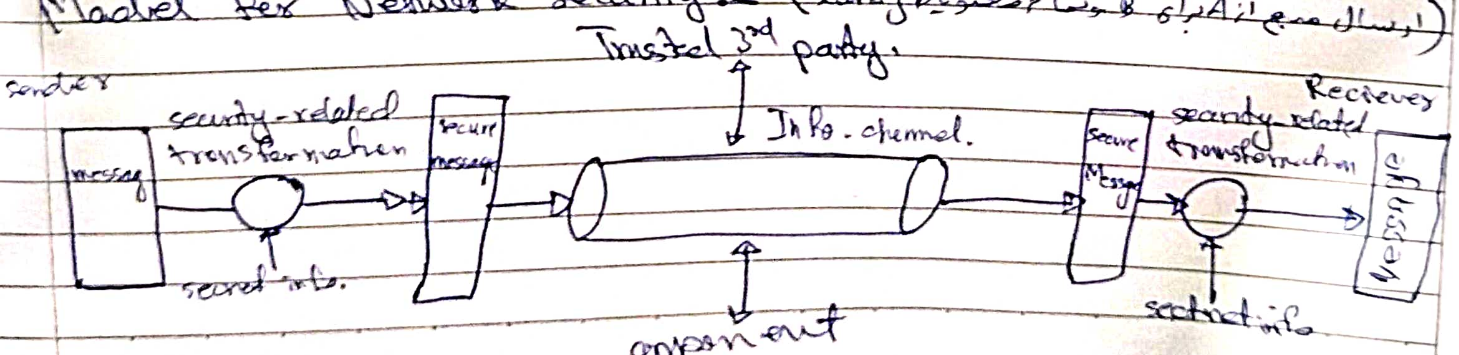
4 basic examples for internet and network security (......)

■ **Computer Security** — A protection afforded ~~by~~ to an automated information system to attain applicable objectives of preserving the confidentiality, availability, integrity, of info. system resources.

- Data confidentiality → Assure private info is protected
- Privacy → Assures the individual control protection of info shared b/w 2 users.
- system work properly and service not denied to user
- → Data integrity: info. and prog. exchanged only in specific and authorized manner.
- → System integ: system perform funct" free from deliberate, unauthorized manipulation of system

Confidentiality:	Integrity:	Availability:	Accountability:	Authenticity:
Preserving restrictions on info access means to protect privacy, information loss of confidentiality is unauthorized disclosure of the system.	Garding against improper info modification & ensuring info and authenticity loss of integrity is the unauthorized modification	Ensuring timely & access, use of info loss of availability is disruption of access or use of info	generates requir" for action to be traced to that entity. It's infosec detection, prevention recovery. (trace source)	being genuine and able to be verified & trusted. verifying "user who they are and verify the trusted sources.

Model for Network Security: (.......)



Teacher's Signature :