STATISTICS

Branch: 16
Node: 38
Linking Phrase: 34
Orphan: 3
Leaf Node: 16
Preposition: 35
Sub Map: 2
Avg Word Per Concept: 1.05

Encryption:Securing Data

Student : 2463831

Used for decipheringthe message

Slide 3 : Cryptograhic Tools

- Encryption:Securing Data → **use of single key for encryption** → Symmetric Encryption
- Encryption:Securing Data → **2 keys used for encryption** → Assymetric Encryption
- Encryption:Securing Data → **means** → The process of encoding thedata with certain value thatit can only be meaningful to only the desired party.

Attack on → **Work as** → Attacking Symmetric Encryption

Symmetric Encryption:
- **also referred as** → Single keyEncryption
- **Works with** → thesecomponents
- **can be implemented** → Encryption Mechanism

Assymetric Encryption:
- **applications** → Digital Envelope, Public Keycertificates, Digital Signature
- **It uses two keys** → Private Key, Public key

Attacking Symmetric Encryption:
- **use of power of computation** → Brute Force Attack
- **decoding the algorithm** → Cryptanalytic Attack

Brute Force Attack → **to prevent Brute force** → Strong Algorithms

Cryptanalytic Attack:
- **can be mitigated with** → Strong Algorithms
- **attacks** → Common Algorithms
- **if successful** → Encryption of all messages

Common Algorithms → **common examples** → AES, DES, TripleDES

Single keyEncryption → **follows** → thesecomponents

thesecomponents:
- **Transmitted** → Cipher text
- **uses Encryption algorithm** → Secret Key used
- **First Step** → Plain Text

Cipher text → **other party gets it** → Decryption Algorithm

Decryption Algorithm → **uses** → Same Secretkey → **gives** → The originalplain text

Encryption Mechanism:
- **Processes block by block data** → Block Cipher
- **processes stream of data** → Stream Cipher

Block Cipher → **one input one at one time** → Reuse of Keys

Stream Cipher → **processes input continuouslyuses pseudorandomkeys** → Fasterperformance

Private Key → **Sender encrypts with their private key** → Requires public key of sender. → **It provides Authentication** → Digital Signature

Public key → **Sender can encrypt withreceiver's pubic Key.** → RequiresPrivate Key of receiver → **provides** → Message Authentication

Message Authentication → **Uses** → Secure Hash Function → **Can be used to block ofany size** → Infeasible to calculate Input fromoutput