ENCRYPTION ALGORITHMS Module 3

ALGORITHMS

SUMMERY

Matched Branch:	0
Partially Matched Branch:	8
Mismatched Branch:	0
Extra Branch:	106
Total Match:	68.42 %
Concept Match:	78.57 %
Link. Phr. Match:	40.0 %
Misconception:	100.0 %
Hierarchy Match:	22.5 %

Grade: 30.23%

including

- Diffie-Hellman Key Exchange Algorithm
  - illustrated by
    - enables two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages
    - limited to the exchange of keys
- Digital Signature Standard (DSS)
  - depicted by
    - provides only a digital signature function with SHA-1
    - cannot be used for encryption or key exchange
- Elliptic Curve Cryptography (ECC)
  - represented by
    - security like RSA, but with much smaller keys
- RSA (Rivest, Shamir, Adleman)
  - characterized by
    - developed in 1977
    - block cipher
    - most widely accepted and implemented approach to public key encryption