

ALGORITHMS

SUMMARY	
Matched Branch:	0
Partially Matched Branch:	8
Mismatched Branch:	0
Extra Branch:	41
Total Match:	31.58 %
Concept Match:	42.86 %
Link. Phr. Match:	0.0 %
Misconception:	91.67 %
Hierarchy Match:	43.33 %

Grade: 27.9%

including

Diffie-Hellman  
Key Exchange  
Algorithm

Digital Signature  
Standard (DSS)

Elliptic Curve  
Cryptography  
(ECC)

RSA (Rivest,  
Shamir, Adleman)

illustrated  
by

depicted  
by

represented  
by

characterized  
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

provides only  
a digital  
signature  
function with  
SHA-1

cannot be  
used for encryption  
or key exchange

security like  
RSA, but with  
much smaller  
keys

developed  
in 1977

block cipher

most widely  
accepted and  
implemented  
approach to  
public key  
encryption