

ALGORITHMS

SUMMERY	
Matched Branch:	0
Partially Matched Branch:	0
Mismatched Branch:	8
Extra Branch:	2
Total Match:	0.0 %
Concept Match:	0.0 %
Link. Phr. Match:	0.0 %
Misconception:	100.0 %
Hierarchy Match:	0.0 %

Grade: 0.0%

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