

DIGITAL SIGNATURES

SUMMARY	
Matched Branch:	0
Partially Matched Branch:	4
Mismatched Branch:	7
Extra Branch:	43
Total Match:	17.65 %
Concept Match:	14.29 %
Link. Phr. Match:	33.33 %
Misconception:	100.0 %
Hierarchy Match:	11.52 %

Grade: 9.74%

illustrated
by

Bob and Alice
confidentially
messaging

Created by
encrypting
hash code
with private
key

Does not provide
confidentiality

Used for authenticating
both source
and data integrity

No one else
has Bob's
private key
and therefore
no one else
could have
created a
ciphertext
that could
be decrypted
with Bob's
public key

Once Alice
receives the
message plus
signature,
the message
hash value
is calculated,
the signature
is decrypted
using Bob's
public key,
and the calculated
hash value
is compared
to the decrypted
hash value

Bob uses a
secure hash
function to
generate a
hash value
for the message
and creates
a digital
signature
by encrypting
the hash code
with his private
key

The message
is unalterable
with access
to Bob's private
key, and so
is authenticated
both in terms
of source
and data integrity

Bob wants
Alice to be
certain that
the message
is from him,
regardless
that the message
need not be
kept secret

Bob sends
the message
with the signature
attached

If the two
hash values
match, Alice
is assured
that the message
must have
been signed
by Bob

such that

message is
safe from
alteration
but not eavesdropping

even in the
case of complete
encryption
the message
can be decrypted
using the
public key