

PUBLIC KEY
ENCRYPTION
REQUIREMENTS

SUMMERY	
Matched Branch:	0
Partially Matched Branch:	0
Mismatched Branch:	9
Extra Branch:	4
Total Match:	33.33 %
Concept Match:	41.67 %
Link. Phr. Match:	0.0 %
Misconception:	100.0 %
Hierarchy Match:	0.0 %

Grade: 11.0%

directly affects

characterized
by

PUBLIC KEY
ENCRYPTION
APPLICATIONS

useful if
either key
can be used
for each role

computationally
infeasible
for the opponent
knowing public
key and cipher
to recover
the original
message

computationally
infeasible
for the opponent
to determine
the private
key from the
public key

computationally
easy to create
key pairs

computationally
easy for the
sender knowing
the public
key to encrypt
messages

computationally
easy for the
receiver knowing
the private
key to decrypt
messages

for instance

digital signatures

public key
certificates

digital envelopes