PUBLIC KEY ENCRYPTION REQUIREMENTS and APPLICATIONS Module 3

PUBLIC KEY ENCRYPTION REQUIREMENTS

SUMMERY

Matched Branch:	0
Partially Matched Branch:	9
Mismatched Branch:	0
Extra Branch:	56
Total Match:	73.33 %
Concept Match:	83.33 %
Link. Phr. Match:	33.33 %
Misconception:	20.0 %
Hierarchy Match:	62.59 %

Grade: 71.88%

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 for the receiver knowing the private key to decrypt messages

computationally easy to create key pairs

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

for instance

digital signatures

public key certificates

digital envelopes