7 Crypto Tutorial

How many keys, in total, are used in an asymmetric/public-key crypto system to pass messages in both directions:
(a) 1
(b) 3
(c) 2
(d) 4

A typical asymmetric/public-key algorithm is:
(a) IDE
(b) IDA
(c) PGP
(d) IDEA

How many keys, in total, are used in the symmetric/private-key system to encrypt messages in both directions:
(a) 1
(b) 3
(c) 2
(d) 4

A typical private-key/symmetric algorithm is:
(a) IDE
(b) IDA
(c) PGP
(d) IDEA

How many possible keys are there with a 16-bit key:
(a) 16
(b) 65,536
(c) 256
(d) 4,294,967,296

How many possible keys are there with a 32-bit key:
(a) 32
(b) 1,048,576
(c) 1024
(d) 4,294,967,296

If it takes 10ns (10×10-9 s) to test a key, determine the amount of time it would take, on average, to decrypt a message with a 32-bit key:
(a) 21.48 seconds
(b) 43 seconds
(c) 21.48 minutes
(d) 43 minutes

Using an asymmetric algorithm, which key does the recipient use to decrypt the main message:
(a) Recipient’s public key
(b) Recipient’s private key
(c) Sender’s public key
(d) Sender’s private key

Using an asymmetric algorithm for authentication, which key does the recipient use to authenticate the sender:
(a) Recipient’s public key
(b) Recipient’s private key
(c) Sender’s public key
(d) Sender’s private key

What bitwise operator is used in encryption, as it always preserves the contentsof the in-formation:
(a) Exclusive-OR'ed
(b) AND
(c) NOR
(d) OR

What happens when a bit-stream is Exclusive-OR'ed by the same value, twice:
(a) Bit-stream becomes all 0's
(b) Bit-stream becomes all 1's
(c) Same bit-stream results
(d) Impossible to predict

If it takes 100 days to crack an encrypted message, and assuming that computing speed increases by 100% each year, determine how long it will take to crack the message after two years:
(a) 25 days
(b) 44.44... days
(c) 50 days
(d) 100 days

If it takes 100 days to crack an encrypted message, and assuming that computing speed increases by 50% each year, determine how long it will take to crack the message after two years:
(a) 25 days
(b) 44.44... days
(c) 50 days
(d) 100 days

If there are only 1024 different passwords for a 64-bit encryption key, what is the key entropy [Hint: Key Entropy = log2 (X) = log10(X)/ log10(2)]
(a) 1024 bits
(b) 10 bits
(c) 64 bits
(d) 18,446,744,073,709,551,616 bits

If there are only 4000 different passwords for a 64-bit encryption key, what is the key entropy:
(a) 64 bits
(b) 11 bits
(c) 11.97 bits
(d) 12.2 bits