Secret Key Crypto Pt 1 Review

What is symmetric key cryptography also known as?

* 5

Describe the basic form of modern block ciphers. What is the feistel cipher? Describe 1 round of feistel encryption and decryption.

* 14, 16, 17

What is the difference between encryption and decryption for a feistel cipher? What is function *f*?

* 22

What is DES? How many bits is the input and output? How many rounds of encryption? How long is the key? How long is the key *really* and why is this? Describe the top level view of DES.

* 24, 25, 26

Describe the initial and final permutations of DES. What is the difference between the 2?

* 27, 28, 30

Describe how the key is processed per round for DES. What is 1 DES round? Describe the Mangler function *f* within the DES round.

* 31, 32, 33, 34, 36

How is 32 bits expanded to 48 bits within *f*? Describe the S-Box.

* 35, 37, 38

What are the overall operations within DES?

* 41

What are the principles for the S-Box design? What is the avalanche effect and what is its place in encryption?

* 45, 46

What is AES? What is the block size? What are the key sizes? Describe the overall encryption process for AES.

* 54, 55

What is the structure of the AES block? Describe the high level view of an AES round. Describe AES decryption.

* 56, 57, 58, 59

Why is secret key crypto more widely used than public key?

* 63