Discussion Questions on Chapters 3, 4, and 5 of "Crypto" by Steven Levy

Feel free to add more questions to this list!

Who was Ralph Merkle? How did he become involved in the development of public key encryption?

Describe the development process and the challenges faced in the implementation of a public key system. What kinds of ideas were proposed?

Who were Ron Rivest, Leonard Adleman, and Adi Shamir? How did they become involved with public key encryption and what did their work lead to?

What was the NSA's role in the development and/or advancement of public key encryption?

Should crypto be kept for the government, or would there be a real need for the general public to use it? What problems surrounded distribution of RSA or other encryption programs to the general public?

Is it possible to keep mathematical ideas secret, or do you think they would eventually be discovered?

Who is Jim Bidzos? How was he involved in the selling of RSA? Was he successful in doing so? What challenges or obstacles did he face?

How did the development of the PC advance the need for crypto?

Discussion Questions on Chapters 1 and 2 of "Crypto" by Steven Levy

Feel free to add more questions to this list!

Who was Whit Diffie? Who was Mary Fischer? What was the relationship (if any) between these two?

How did Diffie's upbringing/background contribute to his desire to learn about cryptography?

Which papers were influential to Whit and why?

Who was Marty Hellman? What did he do? What was his background? How did he come to meet Diffie?

Who was Claude Shannon and how was he involved? Where else have you heard of Claude Shannon's name? Where did he grow up? (You may have to Google this.)

Discuss the development and controversies involved in the development of DES as “the standard”.