Cryptography Questions

Instructions
For this exercise, we will divide into several smaller groups. Each group will have four or five members. And each group will be assigned a specific group of questions. From that specific question group, you will choose one specific question.

At the end of the night, during the exercise presentation, your group spokesperson will introduce your group and speak for one or two minutes on your group's content area. Then, each group member will briefly present the answer to their specific question.

If there is interest, we can post the questions along with their answers.

Best of luck.

Group One, Background, History, and Context
Compare and contrast symmetric and asymmetric cryptography.

1. Explain why: "In secret key cryptography, your secret key is always shared; while in asymmetric key cryptography, your private key is a secret and never shared."
2. Compare and contrast symmetric and asymmetric key lengths and speeds.
3. Construct a table that shows which key in an asymmetric key pair is responsible for which security services.
4. For DES and AES algorithms, construct a table that compares and contrasts their block and key lengths.
5. Define the term "strong cryptography".
6. In a historical context, symmetric cryptography has been limited to well funded, primarily governmental and military, agencies. Explain why.
7. What is the primary limit of asymmetric cryptography?
8. Name and describe each of the four (4) DES modes.
9. Why is DES no longer the Federal Information Processing (FIPs) standard? Give specific dates and events.
10. Briefly list and describe major symmetric and asymmetric algorithms.
11. In addition to DES and AES, name and describe two significant symmetric algorithms.
12. What is the difference between block and stream ciphers? Which is best for hardware implementation? For software implementation?

Group Two, Secure Architecture
Describe Public Key Infrastructure and Kerberos.

1. Describe PKI hardware and software components
2. Define and explain X.500, LDAP, and X.509
3. Compare and contrast the Web of Trust Model used by PGP with the Hierarchal Model used by X.509.
4. Name and briefly describe basic Public Key Algorithms including Diffie-Hellman, RSA, ElGamal, and elliptic curve.
5. Name a specific situation in which you would utilize elliptic curve cryptography.
6. Public Key algorithms are based upon what type of problems?

7. Briefly describe how Kerberos operates. Include major Kerberos components.
8. Compare and contrast cryptographic methods employed by PKI with the cryptographic methods employed by Kerberos.
9. What does Kerberos employ to prevent replay attacks?
10. Describe the relationship between PKI and SSL.

Group Three, Basics
Compare and contrast different hashing methods, and related, methodologies.

1. Compare and contrast major hashing algorithms including MD5 and SHA1 include the length of the hash.
2. Compare and contrast cryptographic methods including MAC, MIC, and HMAC.
3. Describe a birthday hash attack.

Group Four, Secure Protocols and VPNs
Describe the goals and functions of a virtual private network.

1. Compare and contrast SSL, IPSec, L2TP, and PPTP.
2. At what OSI layer do SSL, IPSec, L2TP, and PPTP operate?
3. What key negotiation method does IPSec utilize?
4. What is Internet Key Exchange (IKE)?
5. In an SSL context, what is a rollback attack?
6. In an SSL context, what is a Man in the Middle (MIM) attack?

Group Five, Building Blocks and Basics
List, define, and explain basic cryptographic services, methods and mechanisms include digital signatures, message digests, cryptography, and cryptanalysis

1. Explain how a digital signature works and how it provides security services.
2. In a classical context, define and explain confusion and diffusion (substitution and transposition).
3. What is the purpose of an X.509 public key certificate?
4. Compare and contrast a public key certificate with an attribute certificate.
5. Define and explain the following: Caesar cipher, Scytale cipher, Vigenère cipher, and one time pad.
6. Name the algorithm used by PGP for symmetric encryption.
7. What is a hybrid cryptosystem?
8. What is key escrow?
9. What is the purpose of the Diffie-Hellman algorithm?

Group Six, Basics
For the types of attacks listed below, describe basic cryptanalysis methods be sure to include starting materials and goals.

1. Chosen plain text
2. Chosen cipher text
3. Cipher text only
4. Birthday attack
5. Key clustering