Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 7 of the official CISSP study guide. Here are the top things that you need to know from this chapter on PKI and cryptographic applications.

Understand the key types used in asymmetric cryptography. Public keys are freely shared among communicating parties, whereas private keys are kept secret. To encrypt a message, use the recipient's public key, to decrypt a message, use your own private key, to sign a message, use your own private key, to validate a signature, use the sender's public key.

Be familiar with the three major public key cryptosystems. RSA is the most famous public-key cryptosystem. It was developed by Rivest, Shamir and Adleman in 1977. It depends upon the difficulty of factoring the product of prime numbers. ElGamal is an extension of the Diffie-Hellman key exchange algorithm that depends upon modular arithmetic. Elliptic curve cryptography depends upon the elliptic curve discreet logarithm problem and provides more security than other algorithms when both are used with keys of the same length.

Know the fundamental requirements of a hash function. Good hash functions have five requirements. They must allow input of any length, provide fixed length output, make it relatively easy to compute the hash function for any input, provide one way functionality and be collision resistant. Be familiar with the major hashing algorithms. The secure hash algorithm SHA-3 is the government standard message digest function. SHA-2 supports a variable length message digest ranging up to 512 bits. SHA-3 improves upon the security of SHA-2 and supports the same hash lengths.

Know how cryptographic salts improve the security of password hashing. When straightforward hashing is used to store passwords in a password file, attackers can use rainbow tables of pre-computed values to identify commonly used passwords. Adding salts to the passwords before hashing them reduces the effectiveness of rainbow table attacks. Common password hashing algorithms that use key stretching to further increase the difficulty of attack include PBKDF2, Bcrypt and Scrypt.

Understand how digital signatures are generated and verified. To digitally sign a message, first use a hashing function to generate a message digest, then encrypt the digest with your private key. To verify the digital signature on a message, decrypt the signature with the sender's public key and then compare the original message digest to one you generate yourself. If they match, the message is authentic.

Understand the public key infrastructure PKI. In the public key infrastructure, certificate authorities CAs generate digital certificates containing the public keys of system users. Users then distribute these certificates to people with whom they want to communicate. Certificate recipients verify a certificate using the CA's public key.

Know the common applications of cryptography to secure email. The emerging standard for encrypted messages is the SMI protocol. Another popular email security tool is Phil Zimmermann's pretty good privacy PGP. Most users of email encryption rely on having this technology built into their email client or their web-based email service.

Know the common applications of cryptography to secure web activity. The De facto standard for secure web traffic is the use of HTTP over transport layer security TLS. This approach relies on hybrid cryptography using asymmetric cryptography to exchange an ephemeral session key, which is then used to carry on symmetric cryptography for the remainder of the session.

Know the common applications of cryptography to secure networking. The IPSec protocol standard provides a common framework for encrypting network traffic and is built into a number of common

operating systems. In IPSec transport mode, packet contents are encrypted for peer-to-peer communication. In tunnel mode, the entire packet, including header information is encrypted for gateway-to-gateway communication.

Be able to describe IPSec. IPSec is a security architecture framework that supports secure communication over IP. IPSec establishes a secure channel in either transport mode or tunnel mode. It can be used to establish direct communication between computers or to setup a VPN between networks. IPSec uses two protocols, authentication header AH and encapsulating security payload ESP.

Be able to explain common cryptographic attacks. Ciphertext-only attack require access only to the ciphertext of a message. One example of a ciphertext-only attack is the brute force attack, which attempts to randomly find the correct cryptographic key. Frequency analysis, another ciphertext-only attack counts characters in the ciphertext to reverse substitution ciphers.

Known plaintext, chosen ciphertext and chosen plaintext attacks require the attacker to have some extra information in addition to the ciphertext. The on-path attack fools both parties into communicating with the attacker instead of directly with each other. The birthday attack is an attempt to find collisions in hash functions. The replay attack is an attempt to reuse authentication requests. Those are the study essentials that you need to know for Chapter 7, PKI and cryptographic applications.