# Chapter 5 - Key Topics

| Description | Element | Page | Summary |
|---|---|---|---|
| Ciphers & Keys | Section | 182 | **Cipher** - also called an algorithm, which are rules on how to perform encryption & decryption. **Common Cipher Methods** - Substitution *(character substitution)*, Polyalphabetic *(similar to substitution but with more alphabets)*, Transposition *(many options including letter rearrangement)* **Key** - instructions on how to reassemble characters. For example, a one-time pad (OTP) could encrypt a 32-bit message with a 32-bit key called a pad. **Key Management** - Deals with the relationship between users & keys. Specifically deals with generating keys, verifying keys, exchanging keys, storing keys, and, at the end of their lifetime, destroying keys. |
| Block & Stream Ciphers | Section | 183 | **Block Cipher** - Is a symmetric key pair *(same key used to encrypt & decrypt)* that operates on a group of bits called a block. For example, 32 bits plaintext to 32 bits ciphertext. May add padding for a full block if necessary. Examples, *Advanced Encryption Standard (AES)*, *Triple Digital Encryption Standard (3DES)*, *Blowfish*, *Digital Encryption Standard (DES)*, *International Data Encryption Algorithm (IDEA)* **Stream Cipher** - Is a symmetric key pair *(same key used to encrypt & decrypt)* that operates on a bit at a time against the keystream, called a *cipher digit stream* leading to a ciphertext stream. May have slightly less overhead than a block cipher since it does not require a block. |

| Description | Element | Page | Summary |
|---|---|---|---|
| Symmetric & Asymmetric Algorithms | Section | 184 | **Symmetric Encryption Algorithm / Symmetric Cipher** - uses the same key to encrypt and decrypt the data. Examples, DES, 3DES, AES, IDEA, Blowfish, RC2, RC4, RC5, RC6 **Asymmetric Algorithm** - Is a public key pair. Two keys, *private* and *public* both work in tandem as a pair. The public key is available to anyone who wants to use it, the private key is known only to the device that owns the key pair. RSA (PKCS #1) - with a key length of 512 to 2048, min for security is at least 1024. Slower than Symmetric algorithms but can be used for signing and encryption. Uses integer factorization cryptography. Diffie-Hellman (DH) - allows the negotiation of a shared secret keying material (keys). The algorithm is asymmetric but the keys generated by the exchange are symmetric. ElGamal - is based on the DH exchange. DSA - the Digital Signature Algorithm was developed by the US National Security Agency. ECC - elliptic curve cryptography is public-key cryptography based on the algebraic structure of elliptic curves over finite fields. |
| Hashes | Section | 189 | Used to verify data integrity, also called a digest, message digest, or hash. A cryptographic hash function takes a block of data and creates a small-sized hash value. |
| The three most popular types of hashes | List | 191 | **Message Digest 5 (MD5)** - Creates a 128-bit digest. **Secure Hash Algorithm 1 (SHA-1)** - Creates a 160-bit hash digest. **Secure Hash Algorithm 2 (SHA-2)** - Options of 224-bit digest & 512-bit digest. |

| Description | Element | Page | Summary |
|---|---|---|---|
| Hashed Message Authentication Code (HMAC) | Section | 191 | **Hashed Message Authentication Code (HMAC)** uses the mechanism of hashing with a secret key. Thus, only the other party who also knows the secret key and can calculate the resulting hash can correctly verify the hash. Interception and modification unrealistic since the attacker does not have the secret key. **MD5** is an insecure hash function. **SHA-256** provides adequate protection for sensitive information. **SHA-384** used to protect classified information. |
| Digital Signatures | Section | 192 | Proves that you are who you say you are. **Core Benefits** - Authentication, Data Integrity, Nonrepudiation |
| Digital Signatures in Action | Section | 192 | **Digital Signature** - For example, Batman takes a packet, generates a hash, and then encrypts it with his private key. Batman attaches this encrypted hash ( *digital signature )* to the packet and sends it to Robin. Robin decrypts the packet with Batman's public key and runs the hash function, if a match we know Batman is who he says he is, this is authentication using digital signatures. The keys are exchanged with the certificate exchange, these certificates are trusted if they are signed by a CA they both trust. **Certificate Authority (CA)** - a trusted entity that hands out digital certificates. |
| Description of next-generation encryption protocols | Paragraph | 195 | **Suite B** - algorithms designed to meet future security needs, approved for protecting classified info at secret & top-secret levels. Examples, Elliptic curve cryptography replaces RSA signatures with the ECDSA (EC variant of DSA), DH → ECDH, AES in GaRobin/Counter Mode (GCM), ECC digital signature algorithm, SHA-256, SHA-384, and SHA-512. |

| Description | Element | Page | Summary |
|---|---|---|---|
| Description of IPsec & SSL | Paragraph | 196 | **IPsec** - suite of protocols to protect IP packets. Typically in remote-access VPNs & site-to-site VPNs **SSL/TLS** - typically used for remote-access VPNs & secure communications with web services. |
| Public & Private Key pairs | Section | 199 | A key pair is a set of two keys that work in combination as a team. A public key may be shared with everyone, a private key is known only to the owner. The private key can encrypt, the public key can decrypt and the inverse is also true. This process is also called **public-key cryptography** or **asymmetric key cryptography.** |
| RSA Algorithm, the Keys, & Digital Signatures | Section | 199 | **Keys** - secrets that allow cryptography to provide confidentiality. With RSA digital signatures, each party has a public-private key pair because both parties intend on authenticating the other side. A CA takes each of their public keys as well as their names and IP addresses and created individual digital certificates, and the CA issued these certificates back to each party respectively. The CA also digitally signed each certificate. **Digital Signature** - Batman takes some data, generates a hash, and then encrypts the hash with Batman's private key. This encrypted hash is inserted into the packet and sent to Robin. This encrypted hash is Batman's digital signature. Having received the packet with the digital signature attached, Robin first decodes or decrypts the encrypted hash using Batman's public key. It then sets the decrypted hash to the side for a moment and runs a hash against the same data that Batman did previously. If the hash that Robin generates matches the decrypted hash, which was sent as a digital signature from Batman, then Robin has just authenticated Batman—because only Batman has the private key used for the creation of Batman's digital signature. |

| Description | Element | Page | Summary |
|---|---|---|---|
| Description of Certificate Authorities | Paragraph | 200 | A certificate authority is a computer or entity that issues digital certificates. Inside of digital certificates there contains information about the device. |
| Root Certificates | Section | 202 | A root certificate contains the public key of the CA server and other details about the CA server. Relevant parts of the certificate: **Serial Number** - This is the number issued and tracked by the CA that issued the certificate. **Issuer** - This is the CA that issued this certificate. (Need to have their certificates issued from someone, could be themselves.) **Validity Dates** - These dates indicate the time window during which the certificate is considered valid. **The subject of the certificate** - Includes organizational unit (OU), organization (O), country (C), other details commonly found in an X.500 structured directory. **Public Key** - Contents of the public key and the length of the key. **Thumbprint algorithm and thumbprint** - Hash of certificate. |
| Identity Certificates | Section | 204 | An identity certificate describes the client and contains the public key of an individual host (the client). Identity certificates are used by web servers, APIs, VPN clients, and web browsers (in some cases). **X.500 and X.509v3** - X.500 is a series of standards focused on directory services and how those directories are organized. Example, CN=Batman (CN stands for common name), OU=engineering (OU stands for organizational unit), O=cisco.com (O stands for organization) **Enrollment with a CA** - Authenticate with root CA, request own identity certificate with public-private key pair. CA signs your certificate, you can verify the digital certificate of CA with the signature provided in the authentication step. |

| Description | Element | Page | Summary |
|---|---|---|---|
| Public Key Cryptography Standards | List | 206 | **PKCS #1** - The RSA cryptography standard. **PKCS #3** - The Diffie-Hellman key exchange. **PKCS #7** - A format that can be used by a CA as a response to a PKCS #10 request. The response itself will very likely be the identity certificate (or certificates) that had been previously requested. **PKCS #10** - A format of a certificate request sent to a CA that wants to receive its identity certificate. This type of request would include the public key for the entity desiring a certificate. **PKCS #12** - A format for storing both public and private keys using a symmetric password-based key to “unlock” the data whenever the key needs to be used or accessed. |
| Simple Certificate Enrollment Protocol (SCEP) | Paragraph | 206 | Cisco, in association with a few other vendors, developed the Simple Certificate Enrollment Protocol (SCEP), which can automate most of the process for requesting and installing an identity certificate. |
| Methods to check if certificates have been revoked | List | 207 | **Certificate Revocation List (CRL)** - This is a list of certificates, based on their serial numbers, that had initially been issued by a CA but have since been revoked and as a result should not be trusted. **Online Certificate Status Protocol (OCSP)** - This is an alternative to CRLs. Using this method, a client simply sends a request to find the status of a certificate and gets a response without having to know the complete list of revoked certificates. **Authentication, Authorization, & Accounting** - Cisco AAA services also provide support for validating digital certificates, including a check to see whether a certificate has been revoked. Because this is a proprietary solution, it is not often used in PKI. |
| Untitled | | | |