- Filename: eccouncil-ceh31250-v10-20-1-4-cryptography-concepts
- Show Name: CEHv10 (312-50)
- Topic Name: Cryptography
- Episode Name: Cryptography Concepts Pt.4
- Description: In this episode, Adam and Wes discuss the concepts that help you to understand cryptography.

==========

CEH v10 - Module 20 - Cryptography

First things first - What are the goals of Cryptography?

```
1. Confidentiality
2. Integrity
3. Authentication
4. Nonrepudiation
```

Cryptography Concepts:

Key clustering: different encryption keys generate the same ciphertext from the same plaintext message

Synchronous: encryption or decryption request is performed immediately

Asynchronous: Encrypt/Decrypt requests are processed in queues

Hash function: a one-way mathematical operation that reduces a message or data file into a smaller fixed length output, or hash value

Variable data input (of any size) + hashing algorithm = fixed bit stream output (hash value)

```
• MD5 = 128 bits

• SHA1 = 160 bits
```

Digital signatures: provide authentication of a sender and integrity of a sender's message. A message is input into a hash function. Then the hash value is encrypted using the private key of the sender. The result of these two steps yields a digital signature

Symmetric: A single key used to encrypt and to decrypt

Asymmetric: two different but mathematically related keys are used where one key is used to encrypt and another is used to decrypt

Digital certificate: used to identify the certificate holder when conducting electronic transactions – Type of certificates currently used = X.509 v3

Certificate authority (CA): an entity trusted by one or more users as an authority in a network that issues, revokes, and manages digital certificates

```
• Root CA – only issues certificates to Subordinate CA's

• Subordinate CA – issues certificates to users + computers on behalf of the
```

Root CA

Registration authority (RA): responsible for the accuracy of the information contained in a certificate request. The RA is also expected to perform user validation before issuing a certificate request

Plaintext or cleartext

Ciphertext or cryptogram

Cryptosystem: This represents the entire cryptographic operation. This includes the algorithm, key, and key management functions

Encryption

Decryption

Key or Cryptovariable: The input that controls the operation of the cryptographic algorithm

Non-repudiation

Algorithm

Cryptanalysis: study of techniques for attempting to defeat cryptographic techniques and information security services

Cryptology: the science that deals with hidden, disguised, or encrypted communications

Collision: occurs when a hash function generates the same output for different inputs

Key space: represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password

Work factor: the time and effort required to break a protective measure

Initialization vector (IV): A non-secret binary vector used as the initializing input algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance

Encoding: The action of changing a message into another format through the use of a code

Decoding: The reverse process from encoding – converting the encoded message back into its plaintext format

Transposition or permutation: Swapping/Shifting of blocks of text

Substitution: Changing some part of the plaintext for a different value

Confusion: provided by mixing (changing) the key values used during the repeated rounds of encryption

Diffusion: provided by mixing up the location of the plaintext throughout the ciphertext

Avalanche effect: where a minor change in either the key or the plaintext will have a significant change in the resulting ciphertext

Government Access to Keys (GAK)

What are the Ciphers (algorithms) that I should be aware of?

Symmetric Key Algorithms - are SINGLE KEY !!! - We call that key the PRIVATE KEY | SECRET KEY | SHARED KEY (all or any will do, but make sure that you know we only use one key, shared by all participants in the system)

Weaknesses:

1. key distribution is a challenge / not scalable
2. NO Non-Repudiation possible because everyone has a copy of the key
3. key must be regenerated whenever anyone leaves the group of keyholders

Strength:

```
1. FAST !!! (in comparison to asymmetric)
```

Asymmetric Key Algorithms - are DUAL KEY !!! - We call the keys a PUBLIC / PRIVATE key pair.

Each user has a distinct key pair issued to them upon entry / registration into the system. The PUBLIC key is meant to be shared with anyone who may need it to facilitate communication. The PRIVATE key is kept secret and NOT SHARED.

But, Wait for it .... Wait for it ... Here it comes .. THE UGLY TRUTH:

We use OPPOSITE & RELATED keys in tandem to encrypt & decrypt TA DA!!

So, if your public key is used to encrypt a message, then ONLY your private key can be used to decrypt that message.

That is THE ABSOLUTE HARDEST CONCEPT that you have to master about cryptography. If you can wrap your head around that, and understand whose key is used to do what, you can solve ANY problem or question that you will see.

Strengths:

1. adding users requires ONLY the generation of the key pair for them
2. users can be removed easily, without having to regenerate keys
3. ONLY time you typically regenerate a key is if the PRIVATE KEY of a user has been compromised, or is suspect for some reason
4. provides confidentiality, integrity, authentication and non-repudiation

Weakness:

```
1. SLOW !!! (in comparison to Symmetric)
```

How many keys do I need ?? - n(n-1)/2 keys

participants symmetric keys

```
4                4(4-1)/2 = 6
```

Symmetric Algorithms to know - (DES | 3-DES | IDEA | Blowfish | Skipjack | AES)

Data Encryption Standard (DES) - used to be "the standard" for symmetric encryption for many governments and militaries, but no longer because it is considered compromisable using current computer power.

64-bit block cipher that has five modes of operation. This means that DES takes 64 bits of data and sets them into a block to encipher them into a 64-bit block of ciphertext. DES uses 16 Exclusive ORs (XORs) in a series to generate the ciphertext. We calls these ROUNDS, which is why people say that DES performs 16 rounds of encryption.

NOTE: DES uses a 56-bit key, because 8 bits are supposed to be reserved for parity operations. This means:

```
1. DES = 56 bit key
2. 2-DES (Double DES) = 112 bit key
3. 3-DES (Triple DES) = 168 bit key
```

International Data Encryption Algorithm (IDEA) - Block Cipher like DES. Uses 64-bit blocks to encrypt, like DES. Starts with a 128 bit key, NOT LIKE DES !!

Blowfish - Block Cipher. Uses 64-bit blocks to encrypt, like DES. Variable key from 32 bits to 448 bits.

Skipjack - Block Cipher. Uses 64-bit blocks to encrypt, like DES. 80 bit key. Has an additional capability to use key escrow for the encryption keys. The basis for the U.S. Gov'ts attempts at the Clipper Chip.

Advanced Encryption Standard (AES) - Variable key strengths (128 | 192 | 256 bits) with a 128-bit block. Number of rounds:

```
128-bit key requires 10 rounds
192-bit key requires 12 rounds
256-bit key requires 14 rounds
```

NOTE: The original name for AES is the Rijndael Algorithm. Rijndael consists of four major operations:

```
1. Substitute bytes - Use of an S-box to do a byte-by-byte substitution of
```

the entire block

```
2. Shift rows - Transposition or permutation through offsetting each row in
```

the table

```
3. Mix columns - A substitution of each value in a column based on a function
```

of the values of the data in the column

```
4. Add round key - XOR each byte with the key for that round; the key is
```

modified for each round of operation

NOTE: The Rijndael S-box is a square matrix (square array of numbers) used in the Rijndael cipher. The S-box (substitution box) serves as a lookup table.

CAST - CAST-128 can use keys between 40 and 128 bits in length and will do between 12 and 16 rounds of operation, depending on key length. CAST-128 is a Feistal-type block cipher with 64-bit blocks.

CAST-256 operates on 128-bit blocks and with keys of 128, 192, 160, 224, and 256 bits. It performs 48 rounds and is described in RFC 2612.

Secure and Fast Encryption Routine (SAFER) - either 64-bit input blocks (SAFER-SK64) or 128bit blocks (SAFER-SK128). A variation of SAFER is used as a block cipher in Bluetooth.

Twofish - 128-bit block with keys up to 256 bit length

Rivest Cipher (RC) 5 - Variable block size (32, 64 or 128 bits) with variable key length of 0 bits to 2048 bits.

RC4 - It's a Stream Cipher .... NOT BLOCK !!!

The most widely used stream cipher, being deployed, for example, in WEP and SSL/TLS. RC4 uses a variable length key ranging from 8 to 2,048 bits (1 to 256 bytes).

If RC4 is used with a key length of at least 128 bits, there are currently no practical ways to attack it; the published successful attacks against the use of RC4 in WEP applications are related to problems with the implementation of the algorithm, not the algorithm itself.

NOTE: RC2 is no longer considered to be safe for use, but when active was 64-bit block with a 128 bit key.

Algorithm Block Size (bits) Key Size (bits)

AES 128 128, 192, 256

Rijndael Variable 128, 192, 256

Blowfish 64 32 - 448

DES 64 56

2-DES 64 112

3-DES 64 168

IDEA 64 128

RC2 64 128

RC5 32, 64, 128 0 - 2048

Skipjack 64 80

Twofish 128 1 - 256

Symmetric Key Management - the steps necessary to safeguard keys, including:

```
1. Creation & Distribution - three methods:

    a. Offline Distribution - physical method(s) used to securely deliver the
key to someone

    b. Public Key Encryption - use of Asymmetric encryption to exchange the
symmetric key securely

    c. Diffie-Hellman algorithm - a key exchange algorithm used to enable two
users to exchange or negotiate a secret symmetric key that will be used
subsequently for message encryption. Does not provide for message
confidentiality but is extremely useful for applications such as Public
Key Infrastructure (PKI).



2. Storage & Destruction - Best Practices:

    a. never store the key in the same system as the encrypted data

    b. consider the use of split-knowledge approach for keys



3. Key Escrow & Recovery - Key escrow is a data security measure in which a
```

cryptographic key is entrusted to a third party.

```
    a. Fair Cryptosystem - split knowledge approach with key shards being held
by different trusted third parties
```

Cryptographic Lifecycle - ALL cryptosystems have a limited lifespan based on their ability to withstand attacks. The problem is that technological power keeps advancing, and as a result, what is secure today may be breakable tomorrow. Moore's law is at the heart of this issue and has to be kept in mind when choosing a system, but also as you evaluate the protective ability of the system over the retention period.

Asymmetric Cryptography - uses DUAL KEYS !!! - We call the keys a PUBLIC / PRIVATE key pair.

Each user has a distinct key pair issued to them upon entry / registration into the system. The PUBLIC key is meant to be shared with anyone who may need it to facilitate communication. The PRIVATE key is kept secret and NOT SHARED.

We use OPPOSITE & RELATED keys in tandem to encrypt & decrypt (already said that, but so important, I am saying it again!!)

RSA - most famous asymmetric cryptosystem. Named for its creators:

```
Ron Rivest
Adi Shamir
Leonard Adleman
```

Depends on the computational difficulty of factoring large prime numbers.

Merkle-Hellman Knapsack - developed at approx. same time as RSA, and also based on difficulty of factoring, but took a different approach. Broken in 1984.

El Gamal - based on an extension of the Diffie-Hellman algorithm. Published without a patent, so it is freely available. Doubles the size of any message that it encrypts, which can be an issue.

Elliptic Curve Cryptography (ECC) - based on the elliptic curve discrete logarithm problem. Harder to solve than the factoring problems for RSA or the standard discrete logarithm problem that Diffie-Hellman uses.

Hash Functions - take a message and mix it with a hash to derive a unique output value, the Message Digest. Generated by the sender and sent along with the message to the recipient for two reasons:

```
1. verify the Integrity of the message

2. verify the authenticity of the message (proof of origin & non-repudiation)
```

Note: Message Digests are also called:

```
a. hashes
b. hash values
c. hash total
d. CRC
e. fingerprint
f. checksum
g. digital ID
```

RSA says that a hash function has five basic requirements it must meet:

```
1. input can be of any length

2. output has a fixed length

3. hash function is easy to compute for given input

4. hash function is "one-way"; almost impossible to figure out the input based
```

on the output

```
5. hash function is collision free; almost impossible to find two messages that
```

will produce the same hash value

Hashing Algorithms - Know Them !!!

```
1. Secure Hashing Algorithm (SHA) - variable length input
```

(up to 2,097,152 terabytes) gives fixed output as noted:

```
    a. SHA-160 = 160 bits (using a 512 bit block size for processing the
message data)

    b. SHA-224 = 224 bits (using a 512 bit block size for processing the
message data)

    c. SHA-256 = 256 bits (using a 512 bit block size for processing the
message data)

    d. SHA-384 = 384 bits (using a 1024 bit block size for processing the
message data)

    e. SHA-512 = 512 bits (using a 1024 bit block size for processing the
message data)
```

NOTE: SHA1 is considered to be weak, and has been replaced by the SHA2 series (SHA-224 | SHA-256 | SHA-384 | SHA-512). SHA2 is considered secure, but potentially has same weaknesses as SHA1, so SHA3 has been produced, called the Keccak algorithm.

```
2. Message Digest (2 | 4 | 5) - all produce a 128 bit output

3. Hash of Variable Length (HAVAL) - 128 | 160 | 192 | 224 & 256 bits

4. Hash Message Authentication Code (HMAC) - Variable

5. RIPEMD-160 - output is 160 bits, operates similarly to MD5 on 512-bit blocks
```

Digital Signatures - provide assurance that a message does indeed come from the person who claims to have sent it, it has not been altered, both parties have a copy of the same document, and the person sending the document cannot claim that he/she did not send it.

A digital signature is a block of data (usually a hash) that is generated based on the contents of the message sent and encrypted with the sender's private key. It must contain some unique value that links it with the sender of the message that can be verified easily by the receiver and by a third party, and it must be difficult to forge the digital signature or create a new message with the same signature.

Hence, the reason we use the sender's private key !!!

Digital Signature Steps:

```
1. Cherokee generates a message digest of the original plaintext message using
```

SHA-160

```
2. Cherokee then encrypts ONLY the message digest using her private key - this
```

becomes the digital signature

```
3. Cherokee appends (adds) the digital signature to the plaintext message

4. Cherokee sends the message to Adam (that's me !!)

5. When Adam receives the message, he reverses the process:

6. Adam decrypts the digital signature using Cherokee's public key

7. Adam then uses the same hashing function to create a message digest of the
```

message

```
8. Adam then compares the decrypted message digest to the new one he has just
```

created; if the two match, then the message was sent by Cherokee; if they do not match, then it was not sent by Cherokee

HMAC implements a partial digital signature, guaranteeing the integrity of the message, but does not provide for nonrepudiation

What key to use?

```
1. encrypt a message = recipient's public key

2. decrypt a message = recipient's private key

3. digitally sign a message = sender's private key

4. verify a digitally signed message = sender's public key
```

Digital Signature Standard (DSS) - document that NIST puts out to specify the digital signature algorithms & the encryption algorithms approved for use by the U.S. Federal Government:

```
1. ALL Digital Signatures must use SHA-3 hashing

2. Digital Signature Algorithm for encryption

3. RSA algorithm for encryption

4. Elliptic Curve DSA for encryption

5. Schnorr's Signature Algorithm for encryption

6. Nyberg-Rueppel Signature Algorithm for encryption
```

Public Key Infrastructure (PKI) - comprehensive system required to provide public-key encryption and digital signature services. It has three primary purposes:

```
1. publish public keys/certificates
2. certify that a key is tied to an individual or entity
3. provide verification of the validity of a public key
```

NOTE: PKI functions, or not, based on the TRUST of all of the participants in the system; remove the trust and the system crashes

Digital Certificates - assurance mechanism that allows communicating parties to establish their identity

X.509 v3 is current format most widely used. Part of the X.500 family of standards

Specific information contained in a Digital Certificate:

```
a. Version of conformity (v3)

b. Serial number (unique tracking mechanism from creator)

c. Signature algorithm used to sign the certificate by the Certificate
```

Authority (CA)

```
d. Issuer Name

e. Validity Period

f. Subject's Name (the Distinguished Name, DN, of the owner of the public key
```

in the certificate)

```
g. Subject's Public Key
```

Certificate Authorities (CA) - Perform the activities that make the PKI function, include issuance of certificates and oversight of the certificate lifecycle. The CA “signs” an entities digital certificate to certify that the certificate content accurately represents the certificate owner.

Types of Certificate Authorities:

```
1. Enterprise vs. Stand Alone

2. Root vs. Subordinate
```

Registration Authorities (RA) - assists the CA by verifying the user's identity PRIOR to the issuance of a certificate. DOES NOT ISSUE certificate, but facilitate the CAs ability to do so

Certificate Lifecycle (generation through destruction):

```
1. Enrollment - process of obtaining a certificate from a CA by validating your
```

identity. Will need to provide the CA with a copy of your PUBLIC KEY once identity is validated to allow CA to issue the digital certificate on your behalf. Certificate issued is signed by the CA using it's PRIVATE KEY, certifying that they "TRUST" you and includes a copy of your PUBLIC KEY.

```
2. Verification - the process of checking the validity of an issued certificate
```

by using the issuing CA's PUBLIC KEY. You must also check to ensure that the certificate has not been revoked by consulting the CA's Certificate Revocation List (CRL), or the Online Certificate Status Protocol (OCSP).

```
3. Revocation - the occasional process that a CA engages in to let the world
```

know that the certificate is no longer valid. The revocation request grace period is the maximum response time within which a CA will perform a revocation. Defined by the Certificate Practice Statement (CPS).

Asymmetric Key Management - Control over the issuance, revocation, recovery, distribution, and history of cryptographic keys.

Kerckhoff's principle states: "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

The key is the true strength of the cryptosystem. The size of the key and the secrecy of the key are perhaps the two most important elements in a crypto implementation.

XML Key Management Specification 2.0 (XKMS) - defines protocols for distributing and registering public keys, suitable for use in conjunction with XML Digital Signatures and XML Encryption.

ANSI X9.17 - developed to address the need of financial institutions to transmit securities and funds securely using an electronic medium. Specifically, it describes the means to ensure the secrecy of keys.

Segregation of Duties | Split Knowledge | Dual Control

Key Wrapping and Key Encrypting Keys (KEK) - KEKs are used as part of key distribution or key exchange. The process of using a KEK to protect session keys is called key wrapping. Key wrapping uses symmetric ciphers to securely encrypt (thus encapsulating) a plaintext key along with any associated integrity information and data.

Key wrapping can be used when protecting session keys in untrusted storage or when sending over an untrusted transport medium. Key wrapping or encapsulation using a KEK can be accomplished using either symmetric or asymmetric ciphers.

```
1. If the cipher is a symmetric KEK, both the sender and the receiver will
```

need a copy of the same key.

```
2. If using an asymmetric cipher, with public/private key properties, to
```

encapsulate a session key, both the sender and the receiver will need the other's public key.

Protocols such as SSL, PGP, and S/MIME use the services of KEKs to provide session key confidentiality, integrity, and sometimes to authenticate the binding of the session key originator and the session key itself to make sure the session key came from the real sender and not an attacker.

Pretty Good Privacy (PGP) - Phil Zimmerman created this secure e-mail solution

E-mail security:

```
 1. Secure Multipurpose Internet Mail Extension (S/MIME) - authentication and
```

confidentiality protection through use of public key cryptography and digital signatures. X.509 digital certificates are used for authentication. Two message types:

```
a. signed messages - integrity | sender authentication & non-repudiation

b. enveloped messages - integrity | sender authentication & confidentiality


2. MIME Object Security Services (MOSS) - authentication, confidentiality,
```

integrity & non-repudiation. Uses Message Digest 2 (MD2) and Message Digest 5 (MD5), RSA public key & Data Encryption Standard (DES) for authentication & encryption.

```
3. Privacy Enhanced Mail (PEM) - authentication, confidentiality, integrity &
```

non-repudiation. Uses RSA, DES & X.509

```
4. DomainKeys Identified Mail (DKIM) - assertion that an e-mail was sent by
```

an organization via means of domain name verification. http://www.dkim.org

```
5. Pretty Good Privacy (PGP) - Asymmetric key system using a variety of
```

algorithms including RSA and IDEA

```
6. Opportunistic TLS for SMTP Gateways (RFC 3207) - attempts to setup an
```

encrypted connection with every other mail server that supports it.

Steganography - the ability to use cryptographic techniques to hide information inside of a "cover medium"

Watermarking - the use of steganography to protect documents or Intellectual Property

Digital Rights Management (DRM) - using software to encrypt data and then apply stringent protections to only allow authorized users to interact with the data in specifically defined ways. Types:

```
a. Music
b. E-Book
c. Video Games
d. Document
e. Movies - two technologies:

1. High-Bandwidth Digital Content Protection (HDCP) - content sent over
```

digital connections such as HDMI, DVI and DisplayPort

```
2. Advanced Access Content System (AACS) - Blu-Ray & HD DVD
```

Networking Encryption Applications - Circuit Encryption:

```
1. Link Encryption - protects the entire communication circuit by creating an
```

encrypted tunnel between two end points, encrypting ALL OF THE DATA, including the header, trailer, address and routing information.

```
2. End-to-End Encryption - protects communications between two parties and is
```

performed independently of link encryption. Just encrypts the data payload itself, not any of the routing information, so it is quicker.

```
Higher up in the OSI model = end-to-end  (SSH)

Lower down in the OSI model = link  (SSL/TLS)
```

IP Security Protocol (IPSec) - Most commonly used VPN protocol !!! IP traffic only. Public key cryptography for encryption, access control, non-repudiation & authentication. Two primary components:

```
1. Authentication Header (AH) - authentication, integrity & non-repudiation

2. Encapsulating Security Payload (ESP) - confidentiality with limited
```

authentication. Operates at Layer 3, and can be deployed in either;

```
Transport Mode - IP packet data is encrypted, header is not

Tunnel Mode - Entire IP packet is encrypted & new header is added to manage
```

transmission through the tunnel

Internet Security Association and Key Management Protocol (ISAKMP) - provides security support in IPSec by negotiating, establishing, modifying, and deleting Security Associations (SAs). RFC 2048 lays out four requirements for ISAKMP:

```
1. Authenticate communicating peers
2. Create & Manage security associations
3. Provide key generation mechanisms
4. Protect against threats
```

Security Associations (SAs) - negotiated by ISAKMP during the initialization of an IPSec session. It represents a simplex connection, or a "one-way" transmission agreement. You must have two SAs established to securely communicate, one for each direction of the transmission. If you want to use both AH & ESP bidirectionally with IPSec, then you actually need four SAs !!

Using secure encryption protocols on wireless networks:

Wired Equivalent Privacy (WEP) - uses a predefined and shared symmetric key that is STATIC. Uses RC4 stream cipher. Bad implementation is at the heart of the issues with WEP, not the use of RC4 itself.

```
a. static symmetric key
b. small IV's
```

Wi-Fi Protected Access (WPA) - meant to be a bridge between WEP and newer 802.11i standard that would replace it. Based on Lightweight Extensible Authentication Protocol (LEAP) and Temporal Key Integrity Protocol (TKIP). Also uses a single static passphrase. TKIP sought to improve on WEP by implementing a key mixing function combining the IV with the secret root-key BEFORE using the key with RC4 to encrypt along with a sequence counter to prevent replay attacks and a strong integrity check named Michael.

NOTE: WPA only encrypts traffic between the mobile device & the wireless access point. Once traffic moves to the wired network, it is no longer encrypted by WPA.

Wi-Fi Protected Access 2 (WPA2 or 802.11i) - uses Counter Mode Cipher Block Chaining Message Authentication Protocol (CCMP), based on AES 128 bit key. Can be attacked potentially using a Key Reinstallation Attack (KRACK), which is capable of corrupting the initial 4 way handshake between the client and the Wireless Access Point (WAP), forcing the reuse of keys and/or a key comprised of all zeros.

802.1x / Extensible Authentication Protocol (EAP) - Port based network access control supported by WPA and WPA2. 802.1x actually allows for a "handoff" or integration with additional infrastructure based authentication mechanisms such as RADIUS / TACACS(+), certificates, smartcards, tokens & biometrics. EAP is an extensible and flexible authentication framework used to integrate new authentication technologies.

Protected Extensible Authentication Protocol (PEAP) - EAP encapsulated inside a TLS tunnel

Lightweight Extensible Authentication Protocol (LEAP) - Cisco proprietary alternative for TKIP

Cryptographic Attacks - approaches that seek to exploit one or more vulnerabilities in a cryptosystem to break it

```
    REMEMBER ---> PATTERNS KILL !!!

    REMEMBER ---> IT'S ALL ABOUT THE KEY !!!


1. Analytic Attack - algebraic manipulation attempting to reduce the
```

complexity of the algorithm by focusing on the logic of the algorithm

```
2. Implementation Attack - exploiting weaknesses in the way in which the
```

cryptosystem has been architected & implemented

```
3. Statistical Attack - exploits weaknesses such as floating point errors &
```

an inability to produce truly random numbers

```
4. Brute Force Attack - attempting EVERY POSSIBLE combination until the right
```

one is found

```
Ways to enhance effectiveness of attack:

    a. Rainbow Tables - attempt to shortcut using tables of pre-computed hash
values

    b. Use of specialized hardware

Way to defeat attack:

    a. Salt the passwords - add random values to end of password and then hash.
The salt is stored along with the password hash in the password file
maintained in the O/S. By using the salt value when the password hash is
submitted for verification, we can determine if the password is accurate or
not without exposing it.

    b. pepper - a large constant number stored separately from the hashed
password


    c. key stretching - technique making it more computationally difficult to
guess a password by converting a password to a longer and more random key
for cryptographic purposes such as encryption


5. Frequency Analysis & the Ciphertext Only Attack - what we do when we only
```

have access to the ciphertext of the message. We examine the frequency of letters appearing in the ciphertext attempting to figure out what letters they correspond to in the plaintext version by having knowledge of frequency in the language.

```
6. Known Plaintext - attacker has a copy of the plaintext & ciphertext versions
```

of the same message

```
7. Chosen Ciphertext - attacker can choose which portions of the ciphertext
```

message they decrypt

```
8. Chosen Plaintext - attacker has he ability to encrypt plaintext messages to
```

see what the resulting ciphertext is

```
9. Meet in the Middle - used against algorithms that use 2 rounds of encryption.
```

(reason that 2-DES was defeated) Attacker uses a known plaintext message and encrypts it using every possible key, and then the ciphertext is decrypted using every possible key. When a match is found, the corresponding key pair represents both the encrypt and decrypt capabilities

```
10. Man in the Middle - attacker sits between the two communicating parties,
```

allowing for interception of all communication, including the setup of the communication session. Attacker responds to the sender's initialization request, setting up a secure communication exchange with the sender. The attacker also sets up a secure communication session with the intended recipient, posing as the sender. This allows the attacker to be in the middle and have control of all communications between the two parties

```
11. Birthday Attack (collision attack | reverse hash matching) - find flaws
```

in the one-to-one association of the hash function. Attacker attempts to substitute a digitally signed message that produces the same message digest as the original.

```
12. Replay Attacks - used against cryptosystems that do not use temporal protections.

13. Timing Attacks - based on examining exact execution times of the
```

components in the cryptosystem.

```
14. Rubber-Hose Attack - based on the use of threats or torture to extract
```

needed information.

```
15. Don't Use Hard-Coded Keys (DUHK) Attack - used against hardware/software
```

that implements ANSI X9.31 Random Number Generation

Do Not Forget about Social Engineering !!!