CS 161 Final Cheat Sheet

Kerchoff's Principle

You should not rely on the secrecy of the algorithm/protocol and or keysize, as wall as the possible plain text for security because eventually the adversary will figure them out.

Mono-Alphabetic Ciphers: 1 to 1 mapping of characters to symbols

- Subsitution
  - Shift or Caesar's Cipher $E_k(m) \leftarrow m + k(\texttt{mod}\ N)$ $D_k(c) \leftarrow c - k(\texttt{mod}\ N)$
  - Affine Cipher: $E_k(m) \leftarrow k_! m + k_2(\texttt{mod}\ N)$ $D_k(c) \leftarrow k_!^{-1}(c - k(\texttt{mod}\ N)$
  - Substitution Ciphers have an extreme vulnerability to frequency attacks.

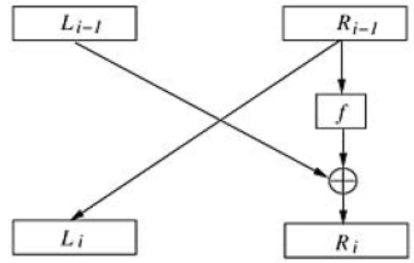
Poly-Alphabetic Ciphers

- Vigenere Cipher: Shift by a repeated key
- Book Cipher (Beale Cipher) key is hidded in a passage of a set book.
- Vernam Cipher
  - Message is m bits and the key is n bits.
  - Bitwise xor the message and the key, if m is greater than n, then use the key multiple times.
- One-Time Pad
  - Same idea as the Vernam Cipher except we use a key that is the same length or greater than the length of the message, then discard it after each use.
- Transposition/Permutation Cipher
  - Break the message into n bit blocks, then on each block perfom the same permutation
  - Despite being polyalphabit, the cipher is still vulnerable to frequency attacks. Because the original patterns are still basically present. You can attack by checking anagrams.

Data Encryption Standard (DES)

DES is a block cipher in which messages are divided into data blocks of a fixed length and each block is treated as one message either in M or in C. The DES encryping and decryption algorithms take as an input a 64-bit plaintext or ciphertext message and a 56-bit key, and output a 64-bit ciphertext or plaintext message. DES is done in 3 steps:

1. Apply a fixed "initial permutation" IP to the input block. $(L_0, R_0) \leftarrow IP(\texttt{Input Block})$ This step has no apparent cryptographic significance.
2. Iterate the following 16 rounds of operations (Feistel Cipher)



- the function is nonlinear and is considered a Substitution Cipher
- the move from $L_i \rightarrow R_{i-1}$ is a Transposition cipher
- Vernam cipher is used at the xor
- k is a 48 bit subsection of the 56 bit, "round key"

Single DES

- vulnerable to brute force or exaustive key search attacks

Triple DES

Triple DES uses an encryption-decryption-encryption scheme,
$c \leftarrow E_{k_1}(D_{k_2}(E_{k_1}(m)))$
$m \leftarrow D_{k_1}(E_{k_2}(D_{k_1}(m)))$
This scheme enlarges the keyspace while maintaining backward compatibility with single DES if $k_1 = k_2$

Advanced Encryption Standard (AES)

AES is a block cipher with variable block size and variable keysize. (block size can be 128, 192, 256 bit)
AES has 4 states:

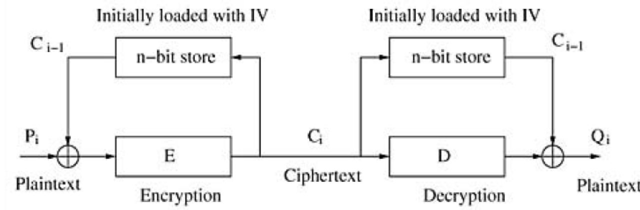
1. Sub Bytes State: nonlinear substitution on each byte
2. Shift Rows State: Transposition rearranges the order of elements in each row
3. Mix Columns State: Polynomial multiplication after converting column to polynomial.
4. Add Round Key State: adds elements of round key to the state, basically bitwise "OR"

Decryption is the inverse of these steps.

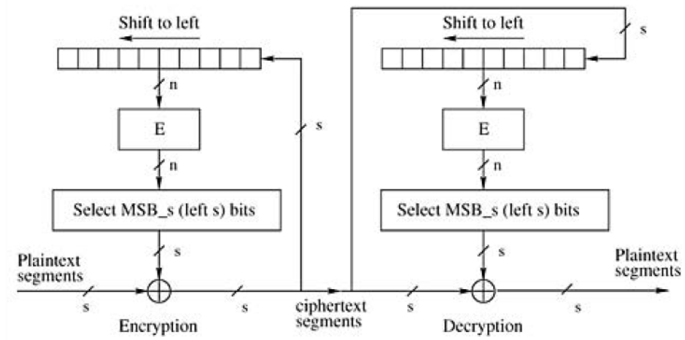
Confidentiality Modes of Operation

Different modes of operation have been devised on top of an underlying block cipher algorithm

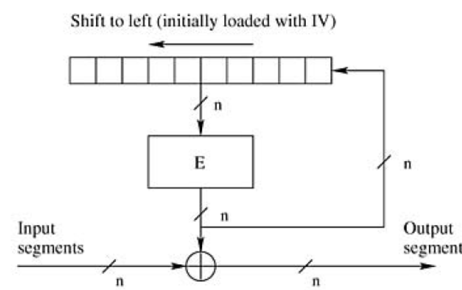
- Electronic Codebook (ECB) Mode This mode encrypts and decrypts every block seperately. It is deterministic and leaves patterns in the cipher text. (for example images.)
- Cipher Block Chaining (CBC) Mode
  - This is the most common mode of operation. In this mode the output is a sequence of n-bit cipher blocks which are chained together so that each cipher block is dependent on all the previous data blocks.
  - Decryption can be done in parallel
  - CBC cannot prived data integrity protection.
  - If the CBC claims data integrity protection, Eve can use (Bomb Oracle Attack) a Decryption Oracle to figure out the padding scheme and eventually the last byte of the cipher text.



- Cipher Feedback (CFB) Mode
  - CFB mode of opration features feeding successive cipher segments which are output from the mode back as input to the underlying block cipher algorithm.
  - CFB requires an IV as the initial n-bit input block



- Output Feedback (OFB) Mode
  - The OFB mode feeds successive output blocks from the underlying block cipher back to it.
  - The feedback blocks form a string of bits which used as the key stream of the Vernam cipher.



- Counter (CTR) Mode
  - The CTR mode features feeding the underlying block cipher algorithm with a counter value which counts up from an initial value. With a counter counting up, the underlying block cipher algorithm outputs successive blocks to form a string of bits. This string of bits is used as the key stream of the vernam cipher, that is, the key stream is XOR-ed with the plaintext blocks. $C_i \leftarrow P_i \oplus E(Ctr_i, i = 1, 2, \ldots, m$ $P_i \leftarrow C_i \oplus E(Ctr_i, i = 1, 2, \ldots, m$

Bomb Oracle Attack

Asymmetric Cryptography

Oneway Trapdoor Function

- Asymmetric crypto system, Public Key Cryptography
- $D \rightarrow R$ is oneway, it is easy to evaluate $\forall x \in D$ and difficult to invert for all values in R.

Textbook Encryption Algorithms

- All or Nothing Secrecy: Given Cipher Text the attacker must not be able to get any information about the plain text
- Passive Attacker: The attacker doesn't modify or manipulate ciphertexts they also don't ask for encryption or Decryption services.

Diffie-Hellman Key Exchange Protocol

`Common Input`	(p, g) `: p is a large prime, g is a generator element in` F_p^*
`Output`	`An element in` F_p^* `shared between Alice Bob.`

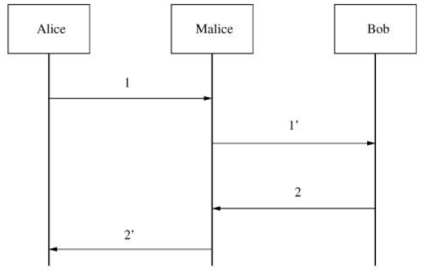
1. Alice picks $a \in U(1, p-1)$; computes $g_a \leftarrow g^a(\texttt{mod}\ p)$; sends g_a to Bob.
2. Bob picks $b \in U(1, p-1)$; computes $g_b \leftarrow g^b(\texttt{mod}\ p)$; sends g_b to Alice.
3. Alice computes $k \leftarrow g_b^a(\texttt{mod}\ p)$
4. Bob computes $k \leftarrow g_a^b(\texttt{mod}\ p)$

Alice and Bob both compute the same key,

$$k = g^{ba}(\texttt{mod}\ p) = g^{ab}(\texttt{mod}\ p)$$

P is a public 2048 bit prime number.

Man in the Middle Attack on Diffie-Helman



1. Alice picks a $\in_u [1, p-1)$, computes $g_a \leftarrow g^a(\texttt{mod}\ p)$ she sends g_a to Malice("bob");
2. (1') Malice("Alice") computes $g_m \leftarrow g^m(\texttt{mod}\ )$ for some $m \in [1, p-1)$; he sends g_m to Bob;
3. (2) Bob picks $b \in_U [1, p-1)$, computes $g_b \leftarrow g^b(\texttt{mod}\ p)$; he sends g_b Malice("Alice");
4. (2') Malice("Bob") sends to Alice: g_m;
5. (3) Alice computes $k_1 \leftarrow g_m^a(\texttt{mod}\ p)$;
6. (4) Bob computes $k_2 \leftarrow g_m^b(\texttt{mod}\ p)$;

Diffie-Helman and the Discrete Logarithm Problem

- Computational Diffie-Hellman Problem
- Discrete Logarithm Problem

Entity Authentication

Entity authentication is a communication process by which a principal establishes alively correspondence with a second principal whose cliamed identity should meet what is sought by the first.

- Host-host type: for example upon a reboot the system must identify to a trusted server neccessary information (like trusted copy of OS, trusted clock setting, or trusted environment settings) Client-Server setting where one host requests certain services from the other server.
- User-Host type: Computer login via telnet/ssh (Authenticated through some password protocol) In serious cases mutual authentication is required.
- Process-host type: used more for distributed computing. Ex. used for "mobile code" or a "browser based" java applet.
- Member-club type: ex a member of a club showing a membership card for access. zero-knowledge identification protocols and undeniable signature schemes

Manipulation Detection Code (MDC)

Lively correspondence

- Freshness
  - Freshness verifies that a message was sent sufficiently recently
  - Data origin doesn't guarantee freshness.
  - This prevents attacks that involve doing large computations on a message or replay attacks.
- nonces
  - A random number, used for verifying a challenge response.
  - Simple example: bob sends a nonce to alice. Alice responds with the encrypted nonce, which was encrypted with a shared private key. If bob recieves the encrypted nonce (in a sufficiently short amount of time) and establishes it was encrypted correctly. This does not provide a proper data-integrity service.
- timestamps

Data Origin Authentication

- Consists of transmitting a message from a purported source (the transmitter) to a receiver who will validate the message upon reception.
- The message validation conducted by the receiver aims to establish the identity of the message transmitter.
- The validation also aims to establish the data integrity of the message subsequent to its departure from the transmitter.
- The validation further aims to establish liveness of the the message transmitter.

Authentication vs Key exchange

- Key exchange or key agreement is usually used during entity authentication or as a subtask

Challenge-response

- Standard vs non-standard (encryption-then-decryption) challenge-response mechanisms
- Standard (as set by ISO, International Organization for Standardization and the IEC, International Electrotechnical Commission) of three challenge-response system.

Unilateral Authentication

- Only one of the two participants is authenticated.

Mutual authentication vs. trusted third-party authentication

- In mutual authentication, both communicating entities are authenticated to each other.
- Originally simply unilateral authentication done twice, once in each direction, until wiener's attack (the Canadian Attack)
- Trusted Third Party (TTP) Authentication requires the principals to use a centralized open system from a trusted third party to authenticate.

Needham-Schroeder password protocol

- Premise: User, U and Host, H have setup U's password entry $(ID_u, f(P * u))$ where f is a one-way function; U memorizes password P_u
- Goal: U logs in H using her/his password.

1. U $\rightarrow$ H : ID_u;
2. H $\rightarrow$ U : "Input password:";
3. U $\rightarrow$ H : P_u;
4. H applies f on P_u, finds entry $(ID_u, f(P_u))$ from its archive; Access is granted if the computed $f(P_u P)$ matches the archived. Where f is a trapdoor function. In the unix password system, f is a series of 25 rounds of DES. Salt (12 bit random number) is used to randomize the flips.

- Data integrity of the password storage file becomes important and the protocol is still vulnerable to online password eavesdropping attack.
- One-time password scheme. In this flawed modification the number of times the hashing function is iterated one more time.

Passwords and salt

Encryted key exchange (EKE)

- The EKE protocol protects the password against online eavesdropping and offline dictionary attacks.
- Premise: User, U and Host, H share a password P_u; The system has agreed on a symmetric encryption algorithm, K() denotes symmetric encryption keyed by K; U and H also agreed on an asymmetric encryption scheme, E_u denotes asymmetric encryption under U's key.
- Goal: U and H achieve mutual entity authentication, they also agree on a shared secret key.

1. U generates a random "public" key E_u, and sends to H: U, $P_u(E_u)$
2. H decrypts the cipher chunk using P_u and retrieces E_u; H generates random symmetric key, K, and sends to U: $P_u(E_u(K))$
3. U decrypts the doubly encrypted cipher chunk and obtains K; U generates a nonce N_u, and sends to H: $K(N_e)$
4. H decrypts the cipher chunk using K, generate a nonce, N_H, and sends to U: $K(N_u, N_h)$
5. U decrypts the cipher chunk using K, and return to H: $K(N_h)$
6. If the challenge-response in 3,4,5 is successful, logging-in is granted and the parties proceed further secure communication

Attacks on authentication protocols

message replay attack

- Malice has previously recorded an old message from a previous run of a protocol and now replays the recorded message in a new run of the protocol
- blocked by freshness

man-in-the-middle attack

Malice intercepts messages between Bob and Alice

parallel session attack

The parallel session attack consists of two or more runs of a protocol executed concurrently under Malice's protection

relection attack

A reflection attack is when an honest principal sends a message to an intended communication partner. Malice intercepts the message and reflects it back at the host

interleaving attack

In an interleaving attack, two or more runs of a protocol are executed in an overlapping fashion under Malic's orchestration. Malic may compose a message and send it out to a principal in one run from which he expects to receive and answer.

attack due to type flaw

Malice uses a flaw, including a principal being tricked to misinterpret a nonce, a timestamp or an indentification into key

attack due to name omission

Name omission is a serious problem that could allow exploits

Kerberos

- single signon
  - Each user memorizes a password, this is the single-signon credential for using the Kerberos system.
- exchanges (authentication service exchange, ticket-granting service exchange, client-server authentication application exchange)
  - Authentication Service Exchange (AS Exchange): runs between a client, C and an "authentication server", AS
  - Ticket-Granting Service Exchange (TGS Exchange): runs between C and a "ticket granting server" TGS after the AS Exchange
    - Checks to see if the difference in time between the client time and host time are within a reasonable range for freshness.
  - Client/Server Authentication Application Exchange (AP Exchange): runs between C and an application server, S after the TGS Exchange
    - The AP Exchange a client, C that uses the newly obtained application session key, to obtain application services fromt he Application Servers
- key distribution center (authentication server, ticket granting server)

SSL/TLS

- Process: *=optional

1. C -¿ S: ClientHello
2. S -¿ C: Server Hello, ServerCertificate*, ServerKeyExchange*, CertificateRequest*, ServerHelloDone
3. C -¿ S: ClientCertificate*, ClientKeyExchange, CertificateVerify*, ClientFinished
4. S -¿ C: ServerFinished

- Hello Message Exchange: Server and Host let each other know what protocols they are capable of running
- handshake with key exchange
- crypto-suite selection, certificates
- use of nonces and random secrets
