Midterm

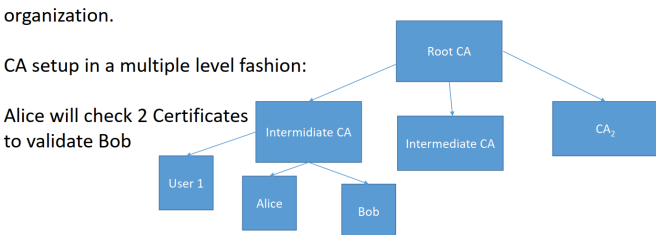
Network --It is a collection of computers (nodes) and transmission channels (links) that allow people to communicate over distances.

- LANs (Local Area Network)
- Wide Area Networks (WAN)s
- Transmission Media: Coaxial Cable, Twisted Pair, Wireless Networks, Fiber Optics(Single mode: Can transmit data at 50 Gbps for 100 km without amplification. Multi mode: fibers have a lower performance is dispersion.), Microwave Line of Sight, Satellites, Low Earth Orbit Satellite, Cellular Systems, Ad Hoc Networks(messages hop from node to node to reach an ultimate destination.), Wireless Sensor Networks, GRID(virtual worldwide computer)
- Open Systems Interconnection (OSI)

Cryptography

$m, c =: E(k_e, m)$
Kerckhoffs' Principle: the security of the encryption scheme must depend only on the secrecy of the key Ke, and not on the secrecy of the algorithm.
Message Authentication Code (MAC) $h(k_e, m)$: h is the MAC function
Bob only accepts messages with:

- proper MAC
- Bob will discard new messages with previous accepted sequence number
  Total Key Exchanges = N(N-1)/2(N people)--(**Public Key Encryption**)Key pair generated by Bob, Public (Pbob) and Private (Sbob). $D(S_{bob}, E(P_{bob}, m)) = m$
  Alice uses Bob's Public key to encrypt m, Bob decrypt the message using his Private or Secret Key. Public key should not be able to be computed from private key.
  Asymmetric encryption(Low performance)
  Digital Signatures Alice generates a key pair (S_{Alice}, P_{Alice}) using a key generation algorithm. Alice publishes Public Key (P_{alice}) Alice computes a signature s and sends it a long with the message m. Bob use v a verification algorithm to check the validity of the received signature using Alice's public key.
  Public Key Infrastructure **Certificate Authority** Bob sends Public Key to CA P_{Bob}. CA send back a Signed Public key encapsulated into a X509 Certificate: The CA will include expiration time, expedition time and the information identifying the CA among other information. Alice obtains (and verify) the CA Public Key from a Database or Bob can send it to her. She can verify Bob's public key using the CA's public key.



attacks:
The Ciphertext-Only Model The attacker tries to decrypt the message by only knowing the ciphertext.
Known-Plaintext Model find encryption key. The attacker will know the plaintext (m) and the ciphertext (c). Attacker can send email to Alice, which generate similar type of reply. Attacker knows the ciphertext and the message.自动回复 & predictable start and end
The Chosen Plaintext model recover the key. Attacker decides plaintext and Cipher values (m,c). So: For plaintext → ciphertext. For ciphertext → plaintext攻击者可以根据其选择的明文来获得对应的密文，从而观察到不同明文对应的密文之间的关系。
The Distinguishing attack goal--A distinguishing attack is any nontrivial method that detects a difference between the ideal encryption scheme and the actual one
other--Authentication and Digital Signature cryptographic functions/ Information leakage or side-channel attacks; in addition to attach the encryption function sampling of the behavior of the encryption process, encryption speed and length.
Generic attacks techniques: Birthday attacks In general if k is the number of inputs and N is the number of outputs there are k(k - 1)/2 input pairs each 1/N chance of being a pair of equal values. If k(k - 1)/2 > N, then likelihood of getting a collision of 50% is $k > n^{1/2}$ So the chance of finding a collision is close to $k(k-1)/2 * 1/N$
The number of elements required to have a collision is $N^{1/2} = k$ or $k = 2^{n/2}$ Known as birthday bound
Meet-in-the-Middle attacks The attacker build a table size $2^{n/2}$ and actively create a MAC. Using this information eavesdrops the messages to try to find a match.
Overall if a key of n=64bits is used to authenticate a transaction, In the standard case: - A collision is expected to be encountered after 2^32 key usages. Attacker will be waiting until this event is observed. Using the Meet in the middle attack more flexible than Birthday attack **If there are N possible values . Two sets of P and Q elements, a collision is expected when PQ/N -> 1**
If P and Q might be close to $N^{1/2}$ (Birthday bound). In some situation is simpler to get elements for one of the sets, as long as PQ is close to N.
Say P is close to $N^{1/3}$ and Q is close to $N^{2/3}$ the attacker could make a list of 2^{40} possible MAC values for the first value and expect to get the first authentication key after listening to only 2^{24} transactions.
Security Level How much work it takes to break a system. if it takes 2^256 steps to work, this corresponds to an exhaustive search for a 256 bit value. A single steps --> single clock cycle. A system needs today needs a 128 bits security level. A secure system should be designed to provide security for 50 years

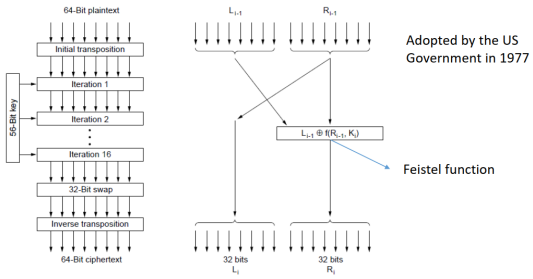
Block Cipher

A block cipher with a block size of k bits specifies a permutation on k-bit values for each of the key values where mn=2^k. A block cipher takes all 2k k bit inputs and maps it into a unique k bit output. 32bit--16GB,64bit 150MTB

- Ciphertext-only attacks: attacker sees only the ciphertext of a message (rare) Chosen-plaintext type:
- Related-key attacks: assumes that the attacker has access to several encryption functions and knows the relationship between their unknown keys.
- Chosen-key attacks: attacker specifies part of the key and then performs a related-key attack.
  The ideal block cipher can be seen as a uniform probability distribution over the set of all possible block ciphers.
- A secure block cipher is one for which no attack exists.
- An attack on a block cipher is a non-generic method of distinguishing the block cipher from an ideal block cipher.
- An ideal block cipher implements an independently chosen random even permutation for each of the key.
  distinguisher The distinguisher algorithm can use any Key for decryption or encryption. Generic if a similar distinguisher is found for almost any block cipher. If the block cipher has an explicit security level of n bits, then a successful distinguisher should be more efficient than an exhaustive search on n-bit.
  Parity and Permutation lookup table example for a single key / block cipher generation
  Real Block Ciphers: A **Round** can be understood as the generation of different repetitions of a week block cipher. Attacks aims blocks ciphers with low number of rounds.奇偶校验（Parity）奇偶校验是一种简单的错误检测技术，常用于存储和传输数据的过程中。在奇偶校验中，每个数据块（如字节）都有一个附加的奇偶校验位，用于检测数据中的错误。奇偶校验位被设置为使数据块中的位数（或字节中的比特数）成为奇数或偶数。例如，如果一个字节中的比特数为奇数，则奇偶校验位被设置为0，使整个字节中的1的数量为偶数。在密码学中，奇偶校验有时被用作一种攻击或区分器，以检测块密码中的某些性质或弱点。
  置换（Permutation）在密码学中，置换指的是对数据的重新排列操作。对于块密码，置换通常应用于数据块的比特级别，以实现加密和解密操作。置换可以通过混淆和扩散来增加密码算法的复杂性和安全性。在块密码的上下文中，一个好的加密算法应该实现独立选择的随机偶置换。这意味着对于每个密钥，加密算法应该生成一个无法预测的、满足偶置换性质的随机置换。一个

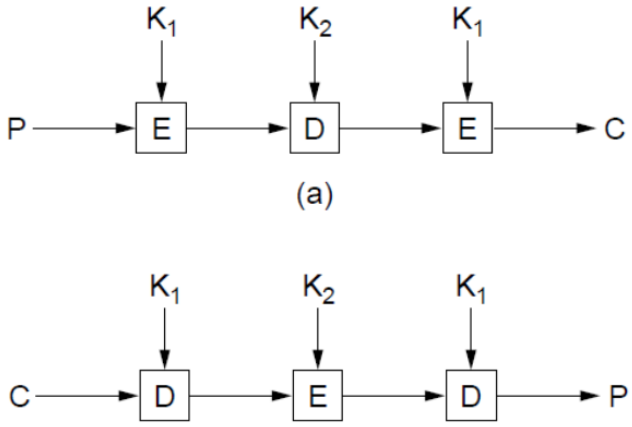
好的置换应该是可逆的（可以通过解密操作逆置换），并且在给定密钥下保证对称性。
Data Encryption System (DES)

(DES)

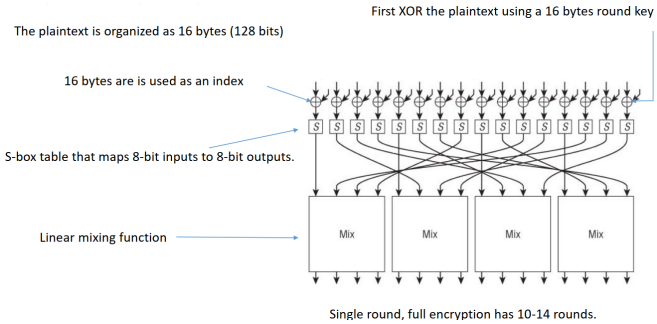


The data encryption standard. (a) General outline. (b) Detail of one iteration. The circled + means exclusive OR.

Triple encryption using DES



Advance Encryption System AES (theoretical not practical)Used to replace DES in the US.
Requirement: Both software and hardware implementations must be possible. The algorithm must be public or licensed on nondiscriminatory terms. The algorithm must be a symmetric block cipher. The full design must be public. Key lengths of 128, 192, and 256 bits must be supported.
Rijndael (AES 2001) Serpent. Twofish. RC6. MARS



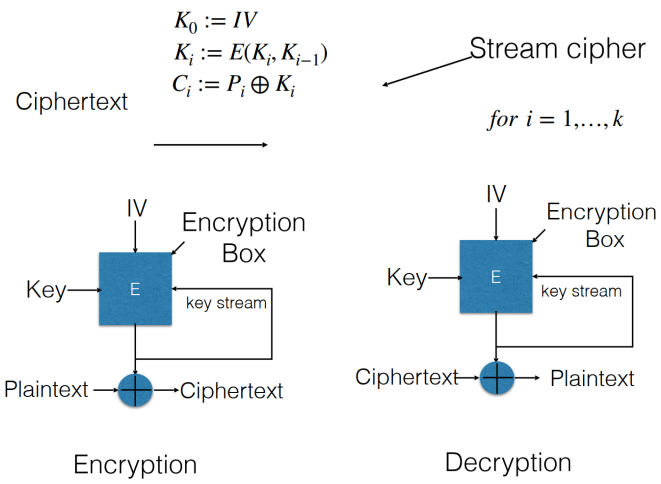
single round |Key size|Round||128|10||192|12||256|14|
Advantages: Parallel operation to perform encryption. Clean design, separating task/functions for each part of the cipher.
Disadvantages: Due to way the decryption is done; inverse lookup table S-box and the inverse mixing operation.
Attacking the cipher 3 to 4 round security margin
|Key size|Round|AttacksRound||128|10|6 to 7||192|12|8||256|14|9| Selection of Rijndael as AES relied on the assumption that future attacks would not give large improvement. Using AES with 128 bit keys 16 round, 192 bit key and 20 rounds and for 256 bit keys 28 round.

Block Cipher Modes

A block cipher mode is a mechanism to encrypt a plaintext P to a ciphertext C for a text and ciphertext with a variably length. Block ciphers encrypt a fixed data block.
Padding Required to uniformly format the length of the plaintext P. Some ciphers require that the length of the plaintext P be an exact multiple of the block size. Padding must be reversible. Padding from simply appending zeros (P||0) until achieving a suitable length NOT reversible. Length of P plaintext string to be padded is < than the length of the padded plaintext
Possible ways to pad a plaintext: If P is plaintext and length of P (bytes). Let b be the block of the cipher (bytes).
1.1 Append single byte with value 128
1.2 Append 0's as needed until the length is multiple of b
1.3 The number of zero bytes added is in the range of 0,…,b-1
Alternative Padding way:
2.1 Find the number of bytes require to pad (n) such:
1 ≤ n ≤ b and n+l(P) is a multiple of b
Pad the plaintext by appending n bytes, each with value n Or,
3.1 Include l(P) at the beginning follow by P then pad to a block boundary.
$k = (l(P) + 1)/b$ Once the plaintext is decrypted the padding needs to be removed. Verification of proper padding elimination so integration needs to be done, to avoid possible authentication issues.

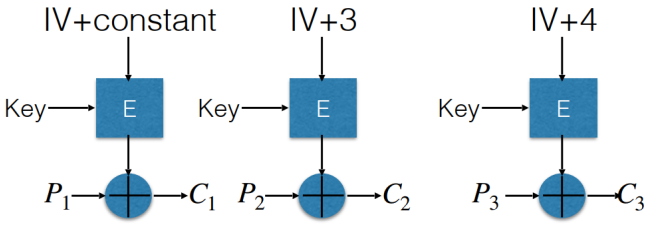
Electronic Code Book (EBC) Simplest method to encrypt a longer plaintext. $C_i = E(K, P_i)$ for i = 1...k (P1=P2 then C1=C2 cause problem)
Cipher Block Chaining (CBC) $C_i = E(K, P_i \oplus C_{i-1})$ for i = 1...k
P if P1 = P2 C1 ≠ C2
C0 ***Initialization Vector (IV)***
Fixed IV *Not used, introduce similar problems as ECB*
Counter IV *IV=0, IV=1,…., not good idea*
Radom IV *If a random IV is used, how the recipient of the message knows about it?*
Solution is to: Random block value C0 for i=1...k and $C_i = E(K,P_i ⊕C{i-1})
$As long as: P1, \ldots, Pk \rightarrow C0, \ldots, Ck The disadvantage is that the ciphertext is one block longer than a plaintext, decryption mechanism is given by: \$P_i := D(K, C_i) \oplus C_{i-1}$
Nonce-Generated IV

1. Unique number NONCE (Number used oNCE) assigned to each message to be encrypted.
   Preparing the message to be send:
2. Message number assignation start 0.
3. Build the nonce using the message number generated. Has to be unique for system and should be as large as a single block of the block cipher.
4. Generated the IV by encrypting the nonce with the block cipher.
5. Using the IV and CBC mode encrypt the message.
6. Verification of the reconstruction of the cipher by aggregating information is needed such the receiver can decrypt the message. Lower number of 32-48 bits compared to a 128 bits if random IV is used. The nonce is secretly transmitted via a pre-established secure channel, nonce should be encrypted using an alternate key if there is a lack of it.
   Output Feedback Mode (OFB) The block cipher is used to generate a key stream, a pseudo random string. 将块密码转化为流密码。OFB模式将一个初始向量（Initialization Vector，IV）输入到块密码中，然后将生成的密文与明文异或，产生密文输出。然后，将上一个密文输出作为下一个输入的初始向量



- 流密码：OFB将块密码转化为流密码，可以处理任意长度的数据。这使得OFB模式适用于实时或流式数据的加密。
- 错误传播：OFB模式中的任何一个比特的错误只会影响对应的密文比特，不会对后续的密文产生扩散效应。这种错误传播特性可以减小错误的影响范围。
- 并行计算：由于OFB模式中的每个块之间没有依赖关系，可以并行地对多个块进行加密或解密操作，提高了加密/解密的效率。
  劣势：- 初始向量的唯一性：初始向量在每个加密会话中必须是唯一的，否则可能会导致安全性问题。
- 密钥流重用：在同一个密钥下，不应该重复使用相同的密钥流，否则可能会导致密码破解攻击。
  Counter Mode (CTR) a stream cipher mode

$$K_i := E(K, Nonce\,||\,i) \quad for\ i = 1,\ldots,k$$
$$C_i := P_i \oplus K_i$$



标准CTR模式 设置

- 消息编号（Message Number）：使用48位值来标识和跟踪消息。它确保每个消息都与唯一的标识符关联。
- 随机数（Nonce）数据：额外使用16位数据来提供更多的随机性和唯一性。随机数通常是一个不会在给定密钥下重复的随机值。
- 计数器（Counter i）：使用64位计数器值，该值从特定值开始，并在每个明文块中增加。计数器值与IV和随机数结合，生成块密码加密的唯一输入。
  在这个设置中，使用单个密钥限制系统可以加密的消息数量为2^48条。每条消息的大小限制为2^68字节，由计数器的大小决定。
  确保IV和随机数的唯一性是为了保证加密过程中的随机性和唯一性。为了满足这个要求，需要选择随机且不会重复的IV和随机数值。如果在相同的密钥下重复使用相同的IV和随机数，会损害加密的安全性，并可能导致密码学的漏洞。
  Chances of a Collision Have a collision or two ciphertext with the same block.
  M is the total blocks encrypted, consider the number of blocks pairs--M(M-1)/2. The chance of each pair of being equal is $M(M-1)/2^{n+1}$ or $M = 2^{n/2}$. n is the block size of the block cipher 2^{-n}
  随机数生成与模式选择：在选择加密模式时，随机数的生成是一个重要因素。CTR模式使用一个初始计数器值与密钥进行加密，并使用计数器的递增值生成密钥流。因此，CTR模式对于产生唯一的、不重复的随机数要求较低。而CBC模式需要一个随机的IV作为初始输入，因此在每次加密会话中，需要生成一个新的随机IV。
  从限制信息泄露的角度来看，Counter Mode（CTR）通常被认为比Cipher Block Chaining（CBC）更高效。在CBC模式中，每个块的加密依赖于前一个密文块，创建了顺序依赖关系。如果两个明文块是相同的，对应的密文块也将是相同的。
  CTR模式通过为每个明文块加密唯一的计数器值将块密码转换为流密码。这意味着每个块可以独立加密，而不依赖于前面的块。CTR模式提供了更好的并行化机会，可以同时加密或解密多个块。CTR模式不会出现错误传播问题，错误只会影响相应的块，而不会影响后续的块。
  与CBC模式相比，CTR模式对某些类型的攻击提供了更好的防护，例如选择明文攻击和填充预言攻击。这是因为CTR模式不涉及明文和密文之间的任何异或操作，使其对这些攻击具有抵抗

性。
无论是CTR模式还是CBC模式，都需要正确的实现和密钥管理才能确保安全性。