Topic 0

CIA

1. Confidentiality
   - Prevention of unauthorized disculosre of information
2. Integrity
   - Prevention of unauthorized modification of information or processes
   - Non-repudiation
3. Availability
   - Prevention of unauthorized withholding of information or resources

Threat model

The description of a class of attacks by:

- The attacker's goals
- The attacker's capabilities

Trade-off in security

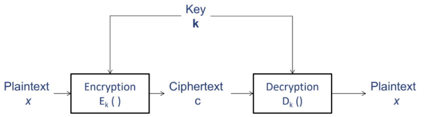
- Ease-of-use: Security mechanisms interfere with working patterns users were originally familiar with
- Performance: Security mechanisms consume more resources and lower performance
- Cost: Security mechanisms are expensive to develop and manage

Threat-Vulnerability-Control

- **Threat**: A set of circumstances that has the potential to cause harm (e.g. an attacker with control of the workstation in the LT could maliciously gather sensitive info like passwords)
- **Vulnerability**: A weakness in the system (e.g. anyone can reboot the workstation from USB or Disk to gain control)
- **Control**: A control, countermeasure, security mechanism is a mean to counter threats (e.g. restrict physical access to the workstation, disable USB booting)
- **A threat is blocked by control of a vulnerability**

Topic 1: Encryption

1.1 Definition: Encryption/decryption/keys



- A symmetric-key encryption scheme consists of encryption and decryption
- A cipher must be correct and secure
  - **Correctness**: For any plaintext x and key k, $D_k(E_k(x)) = x$
  - **Security**: Definition depends on the threat models. Informally, from the ciphertext, teh eavesdropper is unable to derive useful information of the key k or the plaintext x, even if the eavesdropper can probe the system.
- Probabilistic encryption: for the same x, there could be different c's. But they all can be decrypted to the same x.

1.2 Security Model and Requirement

Threat model

- Attacker's goal
  - Total break (most difficult goal)
    - ∗ Attacker wants to find the key
  - Partial break
    - ∗ Attacker may want to decrypt a ciphertext but not interested in knowing the key
    - ∗ Attacker may simply want to extract some info abt the plaintext (e.g. if it is a jpg or excel file)
  - Distinguishability (weakest goal)
    - ∗ With some non-negligible probability of $> 1/2$, the attacker acan correctly distinguish the ciphertexts of a given plaintext from the ciphertext of another given plaintext
- Attacker's capability
  - Ciphertext only attack
    - ∗ Attacker is given a collection of ciphertext c. The attacker may know some properties of the plaintext (e.g. the plaintext is an English sentence)
  - Known plaintext attack
    - ∗ The attacker is given a collection of plaintext m and their corresponding ciphertext c
    - ∗ Attacker might get this as they know the header or part of the plaintext
  - Chosen plaintext attack (CPA)
    - ∗ The attacker has access to an oracle. The attacker can choose and feed any plaintext m to the oracle and obtain the corresponding ciphertext c (all encrypted with the same key). The attacker can access the oracle many times, as long as within the attacker's compute power. He can see the ciphertext and then choose the next input. This black-box is an **encryption oracle**.
    - ∗ e.g. attacker has access to a smartcard
    - ∗ e.g. attacker can eavesdrop
  - Chosen ciphertext attack (CCA2)
    - ∗ Same as CPA but the attacker chooses the ciphertext and the black-box outputs the plaintext. The black-box is a **decryption oracle**.
    - ∗ Padding oracle is a weaker form of a decryption oracle.

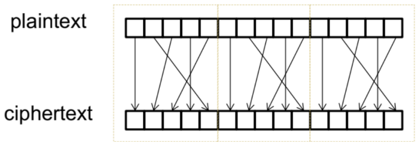
From defender's POV, want a cipher that can protect against the attacker with the highest capability. Cipher is secure against CCA2 (decryption oracle) $\implies$ secure against CPA (encryption oracle)

1.3 Classical ciphers + illustration of attacks

1.3.1 Substitution cipher

- Plaintext and ciphertext are both strings over a set of symbols U.
- The key is a 1-1 onto func from U to U
- Key space: set of all possible keys
- Key space size: total number of possible keys
- Key size/length: number of bits required to represent a key
- Attacks
  1. Exhaustive search (examine all possible keys 1 by 1)
     - Running time depends on size of key space
     - If the table size is 27, the key can be represented by a sequence of 27 symbols. The size of key space is 27!. Exhaustive search eneds to carry out 27! loops, which is infeasible using current compute power.
  2. Known plaintext attack
     - Given sufficiently long ciphertext, the full table can be found
     - Substitution cipher is not secure under known plaintext attack.
  3. Ciphertext only attacker
     - Given that the attacker knows that the plaintext is an English sentence, he can do frequency analysis attack. The frequency of letters used in English is not uniform. Given a sufficiently long ciphertext, attacker may correctly guess the plaintext by mapping frequent characters in the ciphertext to the frequent character in English.

1.3.2 Permutation cipher



- AKA transposition cipher
- First group the plaintext into blocks of t characters, then apply a secret permutation to each block by shuffling the characters
- The key is the secret permutation, which is a 1-1 onto func e from $\{1, 2, \ldots, t\}$ to $\{1, 2, \ldots, t\}$. t can also be part of the key.
- Attack
  - Fails under known-plaintext attack
  - Easily broken under ciphertext only attack if the plaintext is English text

1.3.3 One Time Pad

Properties of xor:

- Commutative: $A \oplus B = B \oplus A$
- Associative: $A \oplus (B \oplus C) = (A \oplus B) \oplus C$
- Identity element: $A \oplus 0 = A$
- Self-inverse: $A \oplus A = 0$

One Time Pad

- Encryption: plaintext xor key bit by bit
- Decryption: ciphertext xor key bit by bit
- Key is only used once, so 1GB of plaintext would need a 1GB key to encrypt
- Security
  - From a pair of ciphertext and plaintext, attacker can derive the key but useless bc key won't be used anymore

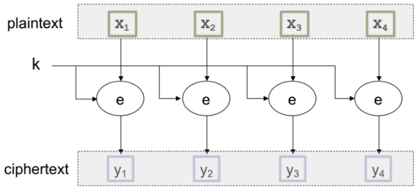
1.4 Modern ciphers + recommended key length

1.4.2 Block cipher & mode of operations

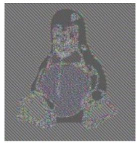
DES/AES are known as block ciphers. Block ciphers have a fixed size of input/output. AES: 128 bits (16 bytes).

Large plaintext is divided into blocks before applying the block cipher.

ECB (electronic code book) mode



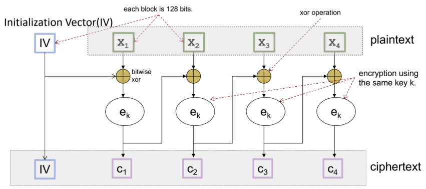
Plaintext

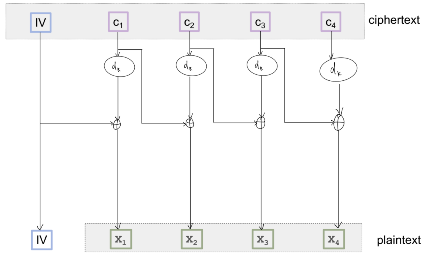


ciphertext

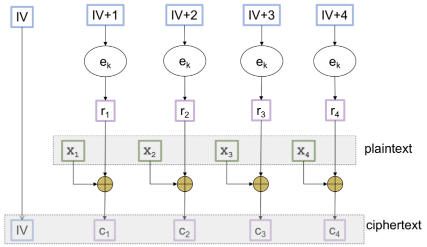
CBC (cipher block chaining) mode on AES

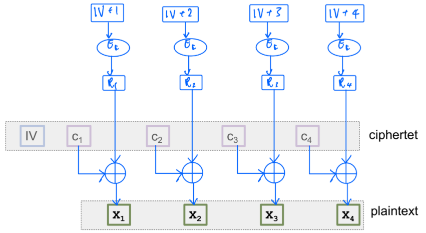
- Initialization vector (IV) is an arbitrary value chosen during encryption, must be different in different encryptions.
- In CBC mode, IV must be unpredictable, else it is susceptable to BEAST attack.
- If IV is randomly chosen, it is unpredictable





CTR (counter) mode



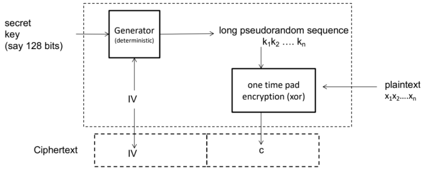


GCM mode (Galois/counter)

Authenticated encryption, ciphertext consists of extra tag for authentication. Secure in the presence of decryption oracle.

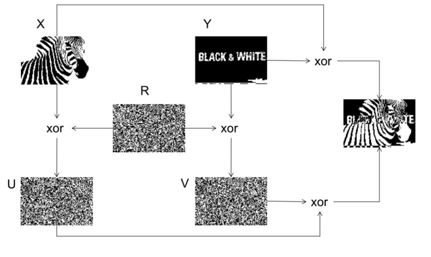
1.4.3 Stream cipher and IVs

Stream cipher is bit by bit. CTR mode is a "stream cipher" but it is not bit by bit.

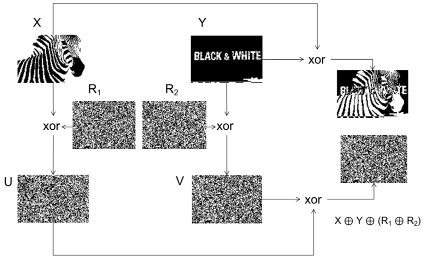


- Need IV and no two IVs can be the same

Stream cipher without IV



Stream cipher with IV

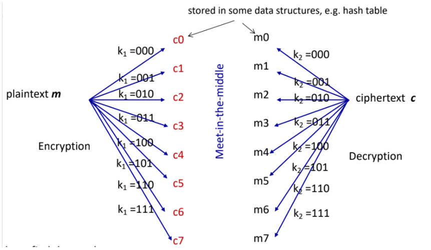


- IV makes an encryption probabilistic

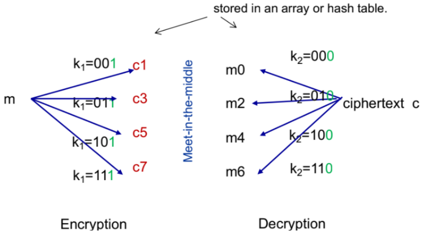
1.5 Examples of attacks on crypto

1.5.1 Meet-in-the-middle

- DES is not secure → improve by encrypting multiple times using different keys
- Consider double encryption under known plaintext attack. Attacker has m and c and wants to know k_1, k_2.
- Using exhaustive search, amount of DES encryption/decryption would be 2^{56+56}
- Hence use meet-in-the-middle attack.
- for k-bit keys, this reduces the number of crypto operations to 2^{k+1}



Tradeoff with time and space

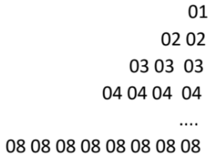


- Last bit of k_1 fixed to 1, last bit of k_2 fixed to 0
- Perform meet-in-the-middle on the first 2 bits of k_1 and k_2

1.5.2 Padding Oracle

Plaintext needs to be padded to split into blocks

- PKCS#7 is a padding standard



01
02 02
03 03 03
04 04 04 04
....
08 08 08 08 08 08 08 08

Padding oracle attack

Attack model:

Attacker has:

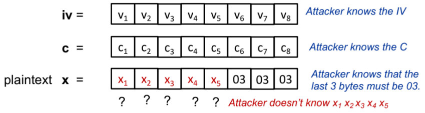
1. Ciphertext (iv, c) where the ciphertext was encrypted using k
2. Access to a padding oracle

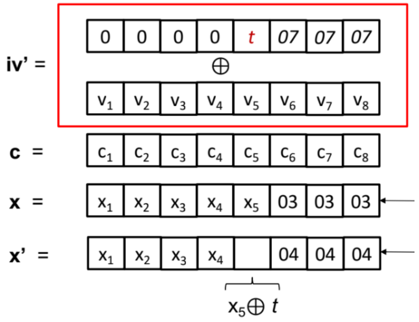
Attacker's goal: plaintext of (iv, c)

Padding oracle input is ciphertext, output is YES if the plaintext is in the correct padding format else NO

Padding oracle attack on AES CBC mode

Attacker knows:





$$iv \oplus d(c) = 03$$

$$iv' \oplus d(c) = 04$$

xor the 2 tgt to get $iv' = 07 \oplus iv$

$$iv' = iv \oplus 00\,00 \ldots t\ 07\ 07\ 07$$

$$d(C_5) \oplus t \oplus V_5 = 04$$

$$d(C_5) \oplus V_5 \oplus t = 04$$

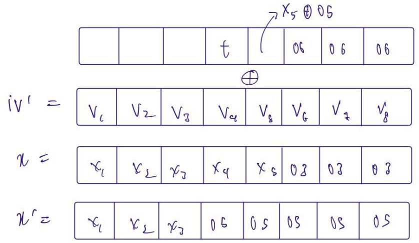
$$d(C_5) \oplus V_5 = x_5$$

$$x_5 \oplus t = 04$$

$$x_5 = 04 \oplus t$$

Keep guessing t until padding oracle outputs YES, then we know x_5

To get next byte:



1.6 Pitfalls in usages and implementations

1. Wrong choice of IV / reusing one-time pad
2. Randomness is predictable
3. Modify existing or design your own encryption scheme
4. Reliance on obscurity: Kerkchoff's principle
   - Kerkchoff's principle: A system should be secure ven if everything about the system, except the secret key, is public knowledge