CS641

Modern Cryptology

Lecture 3

Cryptanalysis

Cryptanalysis is the domain dealing with breaking various encryption algorithms.

- The simplest technique of cryptanalysis is brute-force attack that tries out all possible values of the decryption key.
- While brute-force attack described earlier only needs knowledge of algorithms and ciphertext, and so can always be applied, there are other types of attacks that require additional information.

CIphertext-only Attack

Ela knows a few ciphertexts encrypted with one key.

- Happens due to insecure communication channel.
- Brute-force attack that runs through all possible keys is a type of ciphertext-only attack.

Known Plaintext Attack

Ela knows a few pairs of plaintext and corresponding ciphertext encrypted with the same key.

- Can happen due to carelessness by either Anubha and Braj.
- Stronger attack than ciphertext-only attack.

Chosen Plaintext Attack

Ela can choose a few paintexts for encryption and see corresponding ciphertexts.

- Can happen through an intermediatory between Ela and Anubha.
- Stronger than known plaintext attack.

Chosen Ciphertext Attack

Ela can choose a few ciphertexts and see corresponding plaintexts.

- Can happen when Ela can write messages on the channel for Braj and there is some leakage at Braj's end.
- Stronger than ciphertext-only attack but incoparable to known/chosen plaintext attacks.

Chosen Plaintext and Ciphertext Attack

Ela can choose a few plaintexts and ciphertexts and see corresponding ciphertexts and plaintexts respectively.

- Can happen for a combination of chosen plaintext attack and chosen ciphertext attack scenarios.
- Stronger than all previous types.

Central Axiom

1. Ela has all information that remains fixed, including encryption, decryption, and key generation algorithms.
2. Further, she also has the ability to mount a chosen plaintext and ciphertext attack.

Classical Ciphers under Central Axiom

- Substitution cipher:
  - Ela chooses *abcdef* $\cdots$ *xyz* as plaintext. Corresponding ciphertext yields the key.
  - Even a long enough known plaintext and corresponding ciphertext will yield the key.
- Permutation cipher:
  - Same plaintext and corresponding ciphertext will yield the key.
- Combinations of these ciphers can also be easily broken.

Block Ciphers

A block cipher operates on a fixed size (called blocksize) block of plaintext.

- To encrypt an arbitrary size plaintext m, let $m = m_1 m_2 \cdots m_t$ with $|m_i| = b$ where b is blocksize, $c_i = E(m_i, k_E)$, and $c = c_1 c_2 \cdots c_t$.
- In case $|m_t| < b$, pad it with fixed sequence, for example, 10^*.
- Classical ciphers are all block ciphers, and so are most modern ciphers.

Analysis of Block Ciphers

Brute Force Attack

Send as plaintext all possible 2^b values of a block and collect their ciphertexts to make the correspondence table.

- Requires encryptions of 2^b blocks.
- A type of Chosen Ciphertext Attack.
- Feasible if b is small.
- Therefore, any block cipher with small blocksize is insecure.

Analysis of Block Ciphers

- For secure encryption, we need $b > 120$ bits as per earlier analysis.
- A good choice of b is 128 bits ($= 16$ bytes).
- A large blocksize allows us to mix multiple letters, making frequency analysis also difficult.
- The best mixing is done by a linear transformation, so we can choose E to be a linear transformation.
- To apply linear transformation, we need to view every block as a vector in a certain dimensional space.

A General Linear Transformation Cipher

- Let a block consist of b numbers, with each number limited to certain bitsize.
- This is always possible since any sequence of bits can be viewed as a number.
- Now a block is a b-dimensional vector, say u.
- Let $k_E = (\mathsf{K}, \mathsf{k}_c)$ where K is a $b \times b$ invertible matrix and k_c a b-dimensional vector.

Define $\mathsf{c} = E(\mathsf{u}, k_E) = \mathsf{K} \cdot \mathsf{u} + \mathsf{k}_c$ and $D(\mathsf{c}, k_D) = \mathsf{K}^{-1} \cdot \mathsf{c} - \mathsf{K}^{-1} \cdot \mathsf{k}_c$.

Analysis of Linear Cipher

- Let 0 be all-zero vector and e_i be vector with 1 in i-th dimension and zero everywhere else.
- Send plaintext $0e_1 \cdots e_b$ to Anubha for encryption and let $c_0c_1 \cdots c_b$ be corresponding ciphertexts.
- Then, $c_0 = K \cdot 0 + k_c = k_c$.
- Let the i-th column of K be K_i.
- Then, $c_i = K \cdot e_i + k_c = K_i + k_c$.
- Therefore, $K_i = c_i - k_c = c_i - c_0$.

Analysis of Linear Cipher

- So, any linear cipher can be broken easily with a chosen plaintext attack.
- Even a known plaintext attack can break it as all one needs is linear independence of b plaintext vectors:
  - Suppose plaintext vectors are p_0, p_1, ..., p_b with last b of then linearly independent.
  - Let encryption of p_i be c_i.
  - Then $[c_1 \cdots c_b] = K \cdot [p_1 \cdots p_b] + [k_c \cdots k_c]$.
  - This gives $K = [c_1 \cdots c_b] \cdot [p_1 \cdots p_b]^{-1} + [k_c \cdots k_c] \cdot [p_1 \cdots p_b]^{-1}$.
  - Therefore, $c_0 = [c_1 \cdots c_b] \cdot [p_1 \cdots p_b]^{-1} \cdot p_0 + [k_c \cdots k_c] \cdot [p_1 \cdots p_b]^{-1} \cdot p_0 + k_c$.
  - Above can be used to compute k_c and then K.

Conclusions

#1

Choose large blocksize

#2

E must be non-linear