Introduction to Cryptography

Alvin Lin

January 2018 - May 2018

Stream Ciphers

Stream ciphers were invented in 1917 by Gilbert Vernam. It involves a plaintext x and a key stream k to yield a ciphertext y. Encryption and decryption operations are simple additions modulo 2 (aka XOR).

- Encryption: $y_i = x_i + k_i \mod 2$
- Decryption: $x_i = y_i + k_i \mod 2$

Stream ciphers encrypt bits individually. They're usually small and fast, and are common in embedded devices. Block ciphers on the other hand, encrypt whole blocks of information and are common for Internet applications. The security of stream ciphers depend entirely on the key stream. The key stream k should be random, but reproducible by the sender and the receiver. **Synchronous** stream ciphers use a key stream that only depends on the key, while **asynchronous** stream ciphers use a key stream that also depends on the ciphertext.

Random Number Generators

Random number generators are needed in cryptography, particularly for stream ciphers. There are three types: true random number generators, pseudorandom number generators, and cryptographically secure random number generators. The basic requirements for randomness:

- Uniform Distribution (The frequency of occurrence of ones and zeroes should be approximately equal)
- Independence (Each bit should be uncorrelated with all previous bits)

For cryptography, the compromise of one output must not compromise future or previous outputs.

True Random Number Generators

True random number generators are based on some random physical processes, such as coin flipping, dice rolling, semiconductor noise, radioactive decay, mouse movement, or clock jitter of digital circuits. The output stream should have good statistical properties and should not be able to be predicted or reproduced. These are typically used for the generation of keys and nonces.

Pseudorandom Number Generators

Pseudorandom number generators are algorithms used to produce an open-ended sequence of bits. They generate sequences from an initial seed value. The output stream has good statistical properties and can typically be reproduced and predicted.

The basic requirement when a pseudorandom number generator or pseudorandom function is used for a cryptographic application is that an adversary who does not know the seed is unable to determine the pseudorandom string. The bit stream should appear random even though it is deterministic, and should have no correlation with the seed.

Linear Congruential Generator

The linear congruential generator is an algorithm first proposed by Lehmer parameterized with four numbers $a, b, m, seed$. The sequence of random numbers x_n is obtained via the following iterative equation:

$$x_{n+1} = (ax_n + b) \mod (m)$$

This has bad cryptographic properties due to its linearity.

One-Time Pad

The one-time pad was an improvement to the Vernam cipher propsed by Army Signal Corp officer Joseph Mauborgne. It uses and random key that is as long as the message so that the key does not need to be repeated. The key is used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message.

This scheme is unbreakable because it produces random output with no statistical relationship to the plaintext. The one-time pad offers complete security but has fundamental problems, namely key distribution and key generation. Thus, the one-time pad is useful primarily only in low-bandwidth channels requiring very high security.

Linear Feedback Shift Registers (LSFR)

Linear feedback shift registers are cascades of flip flops, sharing the same clock, whose input bit is a linear function of its previous state. The feedback portion computes fresh input bits by calculating the XOR of certain state bits. Their degree is given by the number of storage elements m, with the maximum output length being $2^m - 1$. Linear feedback shift registers are typically described by polynomials:

$$P(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_2x^2 + p_1x + x_0$$

Single linear feedback shift registers generate highly predictable output. If $2m$ output bits of a linear shift feedback register of degree m are known, the feedback coefficients p_i can be found by solving a system of linear equations. Because of this, most stream ciphers use combinations of stream ciphers.

RC4 Stream Cipher

The RC4 stream cipher was designed by Ron Rivest for RSA Data Security in 1987. The algorithm had been a trade secret, allegedly revealed on the Internet in 1994. The design of RC4 avoids the use of LSFRs and is ideal for software implementation. RC4 generates a keystream (pseudorandom stream of bits), that is used for encryption by combining it with the plaintext using the XOR gate (similar to the Vernam cipher).

- Input: key (typically from 40 to 2048 bits)
- Heart: S-box - a permutation of all 256 possible bytes
- Output: a pseudo-random keystream in bytes

The RC4 cipher has two components, a key scheduling algorithm (KSA) and a pseudo-random generation algorithm (PRGA).