RC4 Security

Rivest Cipher 4 (RC4) is of the most common and earliest stream ciphers. It has been widely used in the SSL and TLS Protocols, WEP, and IEEE 802.11 wireless LAN standard. RC4 has been widespread over the years because of its speed and ease, but it is not risk-free. This report gives a review of RC4 and its security.

Overview of RC4 Encryption

RC4 is a stream cipher created by Ron Rivest for the network security company RSA Security back in 1987. That is why it has also become known as 'Ron's Code.'

Stream ciphers work byte by byte on a data stream. RC4, in particular, is a variable key-size stream cipher using 64-bit and 128-bit sizes. The cipher uses a permutation and two 8-bit index pointers to generate the keystream.

The permutation is done with the Key Scheduling Algorithm (KSA) and then is entered into a Pseudo-Random Generation Algorithm (PRG), which generates a bitstream. The pseudorandom stream that the RC4 generates is as long as the plaintext stream. Then through the Exclusive Or (X-OR) operation, the stream and the plaintext generate the ciphertext.

Working of RC4

Encryption Procedure

1. The user inputs a plain text file and a secret key.
2. The encryption engine generates the keystream using KSA and PRGA algorithms.
3. This keystream is now XOR with the plaintext. This XORing is done byte by byte to produce the encrypted text.
4. The encrypted text is then sent to the intended receiver, the intended receiver will then decrypt the text, and after decryption, the receiver will get the original plain text.

Decryption Procedure

- Decryption is achieved by doing the same byte-wise X-OR operation on the ciphertext, since (A XOR B) XOR B = A, the byte-wise XOR operation on ciphertext with keystream results in the plaintext.

Applications of RC4 Encryption

RC4 gained massive popularity and had standard implementations in commercial applications over the years. It has been known for being a speedy, uncomplicated, and affordable encryption method.

The main advantages of RC4 include simplicity of implementation and use and the speed of operation and deployment. It allows working with massive data streams in an efficient and fast way. RC4 stream ciphers are also light in terms of memory use.

RC4 Vulnerabilities

Despite RC4's wide range of advantages, numerous vulnerabilities have been identified. As a result, it is now considered insecure as a form of encryption and is more and more rarely used.

For example, since RC4 is a stream cipher and not a block cipher, so it is more vulnerable to a bit-flipping attack. RC4 has also been found to be susceptible to plaintext recovery attacks and several other security risks.

Here are the most prominent RC4 issues and attacks identified over the years:

- **Weak keys in RC4:** Weak keys are the small set of keys in RC4, which leaves some traces in the keystream generated after KSA or in the output bytes after PRGA. If intruders follow such traces, they can quickly recover the key from the internal state or the output stream.
- **Biased** bytes: In stream ciphers, the event or bytes are said to be biased if an event occurs with a different probability from the uniformly random sequence of bits/bytes. Studying the non-random behaviour of bytes is the goal of the attacker. Several biases or correlations related to the secret key, state variables, and short-term and long-term biases related to keystream bytes exist in RC4 KSA and PRGA.
- **Distinguishers:** If the events in RC4 are biased and are solely based on keystream bytes, then such biased events are referred to as distinguishers.
- Key collisions: In RC4 KSA, it may be possible to generate a similar state even if two different keys are used, and a similar output keystream will be produced. Such a scenario is known as a key collision or related key pairs. The construction of such key pairs is the goal of the attacker.
- **Key recovery from the** state: RC4 PRGA is reversible in nature. From any given state of PRGA, it is easy to reach the internal state, and it is pretty easy to recover the secret key from the internal state.
- **Fluhrer Mantin Shamir attack:** The first bytes of RC4 keystreams are not random and thus expose information about the key, which opens the doors for WEP attacks.
- **Andreas Klein attack:** Correlations between the key and the RC4 keystream were discovered.

Sakshi Shashikant Yeole – 20CS01047