Alan Kuri

Ricardo Rodríguez

Alan Macías

A5

1: Still in use?

Yes

2: Has it been attacked or broken?

It has been proved to be vulnerable several times. There was actually a demonstration in 2006 that showed that A5 was easily broken and messages could be read almost in the moment.

3: Is it successful? Where?

It is used in the GSM (Global System for Mobile communications) standard to proportion message “privacy”.

4: How does it work?

GSM sends groups of 114 bits. For each group, A5 generates another bit sequence and applies and XOR to the GSM group. A5 consists of 3 shift registers that are modified during several clocking cycles. After the cycling is done, the 114 bits of output of A5 are XORed with the text to encrypt/decrypt it.

RC4

1: Still in use?

Yes, but in systems for common use. In modern systems because of the high security standards it was excluded.

2: Has it been attacked or broken?

It was broken in 1994 the description of the algorithm was posted in the email of Cypherpunks. Then to the email group of sci.crypt. And after that, post on various internet sites.

3: Is it successful? Where?

It was successful in the Transport Layer Security (TLS/SSL) to protect the Internet traffic. Also in Wired Equivalent Privacy (WEP) is successful in adding security to the Wireless Networks.

Used in:

- SSL/TLS (Secure socket, transport layer security) between web browsers and servers.
- WEP(Wired Equivalent Privacy).
- WPA default
- Bittorrent Protocol Encryption
- Microsoft Point-to-Point
- Remote Desktop Protocol.

4: How does it work?

Consists in 2 algorithms, 1-Key Scheduling Algorithm(KSA) and 2-Pseudo Random Generation Algorithm (PRGA). Both algorithms use a 8-by-8 box (is an array of 256 numbers). The KSA make the first step in the S-box array fill the array and another array let's call it A its filled based on the seed in it. Once both arrays are full, the S-box is exchange based on the seed, that generates the key.

SEAL

1: Still in use?

Yes

2: Has it been attacked or broken?

Yes. In 1997 it was shown that the output stream could be distinguished from random after seeing roughly 2^34 bytes of output

3: Is it successful? Where?

Since it is one of the fastest stream cipher algorithms it can be an option, but not a single source affirms that it is successful for something in particular, it is only mentioned that it is optimised for machines with a 32-bit word size .

4: How does it work?

The output stream is generated in rounds. In each round, a function is applied to the current state using the round keys. The new state (which changes for each round) is then masked by some entries in a mask table and this value is output as a part of the stream.

References

https://asecuritysite.com/encryption/a5

https://www.researchgate.net/figure/The-A5-1-stream-cipher-algorithm_fig1_267819492

https://eprint.iacr.org/2002/019.pdf