MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

ORYX STREAM CIPHER – PART 3 (REVISED)

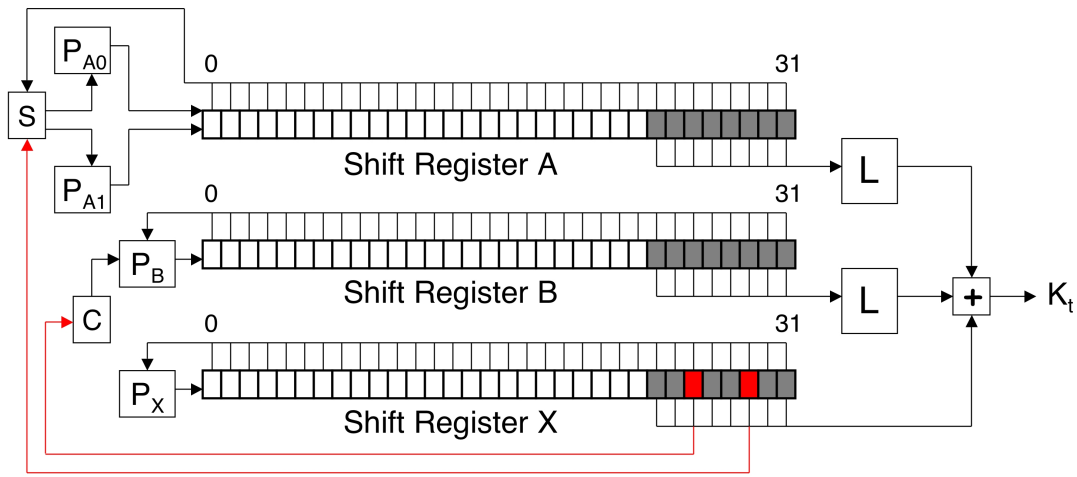
Authors: Mark Stamp, Richard M. Low

May 2013

Introduction

ORYX is a stream cipher that was developed as part of a U.S. cell phone industry security standard. The system was deployed and briefly used in the late 1990s until its many security flaws became apparent [1].

The internal operation of the ORYX cipher is illustrated below, where K_t is a keystream byte that is XORed with a plaintext byte to encrypt, and XORed with the corresponding ciphertext byte to decrypt.



The definitions of P_X, P_{A0}, P_{A1}, P_B, S, C, and L are given in [2], and they also appear in the simulator `ORYX.c`. Note that L is a lookup table where $(L(0), L(1), \ldots, L(255))$ is a permutation of the byte values $\{0, 1, 2, \ldots, 255\}$.

Challenge

The challenge here is to recover the initial fill of the B register and as much of the unknown permutation as possible, given the initial fills of A, X, and the first 50 keystream along with the corresponding values of $\mathrm{L}(\mathrm{H}(\mathrm{B}))$. Since each keystream byte involves 2 elements of the L permutation, at most, you will only be able to determine 100 elements of the table L.

The known fills are

$$A = \texttt{deadbeef} \quad \text{and} \quad X = \texttt{1c6f2726}$$

The first 50 keystream bytes are

```
3f ff dc 91 cd 06 ff 5f 44 7d 83 5a 96 4c 44 2d c8
f3 22 9e 4f a1 21 1d d1 8e a4 e2 1f 76 da 12 ba 68
a9 13 e1 87 12 7c 40 57 c7 89 84 f3 a0 b5 08 01
```

and the corresponding $\mathrm{L}(\mathrm{H}(\mathrm{B}))$ values are

```
b4 5d df 68 8b c6 5b 7c 8f 0a b1 f9 8f fb b1 a6 2e
fa 0a 12 11 07 4e 5a 2f 3e dd 21 e3 2d 73 d7 1a 2a
01 1c 26 fd 0e 53 43 f0 95 8e 3d ce ad ed ce 9f
```

For your solution, give the initial fill of B followed by a space and attach the entries of the 16×16 table of the L permutation separated by a space, with any unknown values of L denoted as `xx`. Make sure to write all values in hex.

For example, suppose that you determine the initial fill of the B register is fedcba98 and $L(i) = i$, for $i = 0, 1, \ldots, 85$, with the remaining L entries being unrecoverable. Then your solution would be submitted as

```
fedcba98
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f
20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f
30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f
40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f
50 51 52 53 54 xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
```

References

[1] G. Rose, *Authentication and security in mobile phones*, 1999
https://opensource.qualcomm.com/assets/pdf/AUUG99AuthSec.pdf

[2] M. Stamp and R. M. Low,
Applied Cryptanalysis: Breaking Ciphers in the Real World,
Wiley-IEEE Press, 2006

Acknowledgments

We would like to thank George, Viktor, Jomandi, and Yokozuna, who are four committed MTC3 users. They have greatly supported us with the revision of this challenge so that you are now able to find a unique solution.