MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

ORYX STREAM CIPHER – PART 4B

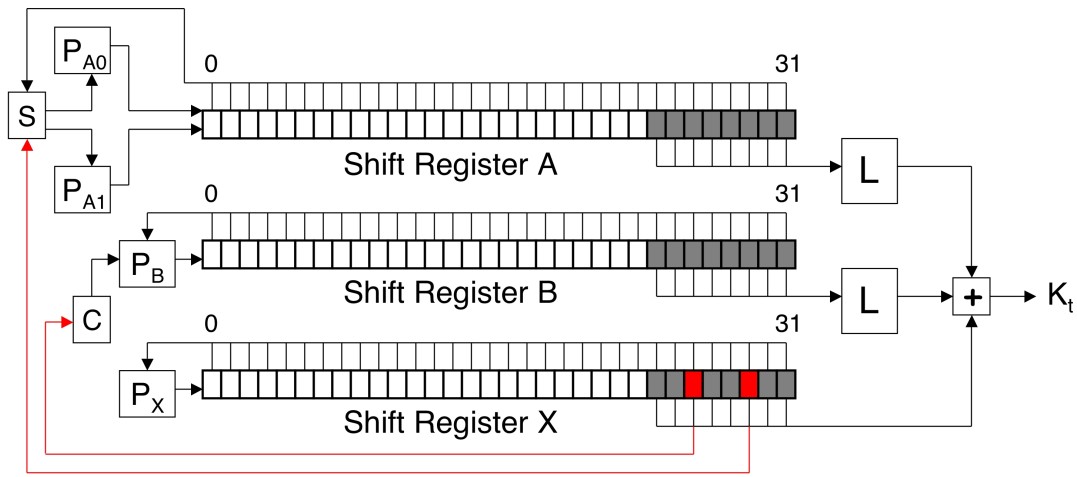
Authors: Mark Stamp, Richard M. Low

March 2014

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 fills of the shift registers X, A, and B, as well as the unknown L permutation. You are given the first 750 bytes of keystream and the first 128 (out of 256) elements of L, which appear, in hex, in the file `oryx4b.txt`. Give your solution in the form

X initial fill
A initial fill
B initial fill
L permutation

where all values are in hex and the L permutation is given as a 16×16 table.

For example, if you determine that the initial fill of each register is fedcba98 and L is the identity permutation, then your solution would be submitted as

```
fedcba98
fedcba98
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 55 56 57 58 59 5a 5b 5c 5d 5e 5f
60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f
70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f
80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f
90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f
a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf
c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf
d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df
e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef
f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff
```

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