MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Typex – Part 1

Authors: Kelly Chang, Richard M. Low, Mark Stamp

February 2013

During World War II, the British used a cipher machine known as Typex that was based on the commercial version of the Enigma cipher [1].

One major difference between Typex and a 3-rotor Enigma machine is that the former uses a pair of static rotors (called stators) in place of the Enigma stecker (called plugboard). Another significant difference is that each Typex rotor has multiple notches, which cause it to step multiple times per revolution of its adjacent rotor. In contrast, the Enigma rotor stepping is essentially odometer-like. Also, each Typex rotor can be inserted in a forward or reverse orientation – like Sigaba rotors, but unlike Enigma rotors – which effectively gives twice as many rotors to choose from [2].

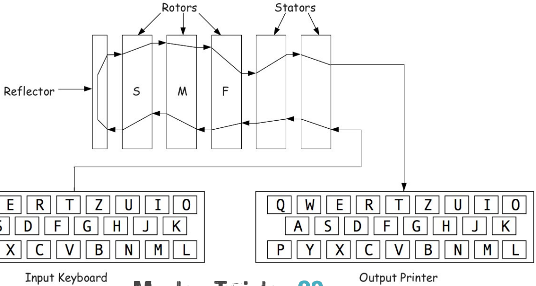
Another minor difference is that the word-space character is allowed in Typex plaintext messages. Before encrypting, each space is mapped to the letter X. Consequently, if we use Typex to encrypt

THE QUICK BROWN FOX

it would decrypt as

THEXQUICKXBROWNXFOX

The internal operation of the Typex cipher is illustrated below.



Challenge

The challenge here is to conduct a known-plaintext attack on a Typex-encrypted message and to recover the key. For this problem, there are 8 known rotors with known notch positions, as given in the `Typex.c` simulator code. The key consists of selecting 5 distinct rotors (3 for use as rotors and 2 as the stators), putting the 5 selected rotors/stators in order, selecting the orientation of each of the 5 rotors/stators, and setting the initial position of each selected rotor/stator.

In your solution, give the key in the same format as used when running the simulator. For example, the key

```
71625 01010 ZWABA
```

has the following meaning:

rotor/stator	number	orientation	initial position
left (slow) rotor	7	forward	Z
middle (medium) rotor	1	reverse	W
right (fast) rotor	6	forward	A
left stator	2	reverse	B
right stator	5	forward	A

For this challlenge, the ciphertext is given by

```
KXWCKMIWRSHTJVDJRVYYFSYYWWRZPVOROKRRNXYCVATDNGWTDOQNBRJC
QPBFOOZXHSJRPSTLDMUBSUTDAQRPZEHCPFTCIYENOUTSMWBISCNLUHLA
CIQPXQDNJFAOMYUNEERSZAKQJEQKKMEBFOTANYHYRFDJTVKCIGPTWCPY
```

and the corresponding plaintext is

```
WE SHALL FIGHT ON THE BEACHES WE SHALL FIGHT ON THE LAND
ING GROUNDS WE SHALL FIGHT IN THE FIELDS AND IN THE STRE
ETS WE SHALL FIGHT IN THE HILLS WE SHALL NEVER SURRENDER
```

References

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

[2] K. Chang, R. M. Low, and M. Stamp, Cryptanalysis of Typex, to appear in *Cryptologia*

[3] http://en.wikipedia.org/wiki/TypeX

[4] http://www.cryptomuseum.com/crypto/uk/typex/index.htm