4 Other Applications of Running-Text Analysis

Key Re-Use

Consider an alphabet Σ with a group structure, and consider an (aperiodic or periodic) polyalphabetic cipher that uses the CAESAR operation: For a plaintext $a = (a_0, a_1, a_2, \ldots)$ and a keystream $k = (k_0, k_1, k_2, \ldots)$ the ciphertext $c = (c_0, c_1, c_2, \ldots)$ is given by

$$c_i = a_i * k_i \quad \text{for } i = 0, 1, 2, \ldots.$$

Because the key is not necessarily meaningful text the cryptanalytic methods for running-text ciphers don't apply.

But suppose another plaintext $b = (b_0, b_1, b_2, \ldots)$ is encrypted with the *same* key k, resulting in the ciphertext $d = (d_0, d_1, d_2, \ldots)$,

$$d_i = b_i * k_i \quad \text{for } i = 0, 1, 2, \ldots.$$

The attacker recognizes this situation by coincidence analysis.

Then the difference (or quotient, depending on the notation of the group law) is given by

$$d_i * c_i^{-1} = b_i * k_i * k_i^{-1} * a_i^{-1} = b_i * a_i^{-1} \quad \text{for } i = 0, 1, 2, \ldots.$$

In this way the attacker who knows the ciphertexts c and d finds the difference $b_i * a_i^{-1}$ that is the composition of two meaningful texts she doesn't know but wants to. She therefore applies the methods for running-text encryption and eventually finds a and b and then even k.

Historical Notes

This kind of analysis was a main occupation of the cryptanalysts in World War II and in the following Cold War. In particular teleprinter communication used additive stream ciphers (mostly XOR) with keystreams from key generators and very long periods. In case of heavy message traffic often passages of different messages were encrypted with the key generator in the same state. Searching such passages was called "in-depth-analysis" and relied on coincidence calculations. Then the second step was to subtract the identified passages and to apply running-text analysis.

Some known examples for this are:

- Breaking the Lorenz cipher teleprinter SZ42 ("Schlüsselzusatz") by the British cryptanalysts at Bletchley Park in World War II (project "Tunny").

- Breaking HAGELIN's B21 in 1931 and the Siemens-Geheimschreiber T52 in 1940 by the Swedish mathematician Arne BEURLING. The T52 was also partially broken at Bletchley Park (project "Sturgeon").

- The latest politically relevant application of this cryptanalytic technique occurred in the 1950es. US cryptanalysts broke Sovjet ciphertexts and by the way debunked the spy couple Ethel und Julius Rosenberg (project "Venona"). The Sovjet spys used a one-time pad—in principle. But because key material was rare keys were partly reused.

Large Periods

Another application is the Trithemius-Belaso cipher with a large period l, large enough that the standard procedure of arranging the ciphertext in columns and shifting the alphabets fails.

Then the attacker may consider the ciphertext shifted by l positions and subtract it from the original ciphertext:

$$c_{i+l} - c_i = a_{i+l} - a_i.$$

Or, if the key consists of meaningful text, directly treat the cipher as a running-text cipher.

Exercise.

```
BOEKV HWXRW VMSIB UXBRK HYQLR OYFWR KODHR JQUMM SJIQA THWSK
CRUBJ IELLM QSGEQ GSJFT USEWT VTBPI JMPNH IGUSQ HDXBR ANVIS
VEHJL VJGDS LVFAM YIPJY JM
```

Hints.

- Find evidence for a period of 38 or 76.
- Try the probable word `AMERICA` as part of the key.