The affine cryptosystem

$$f_E: \mathbb{Z}_N \to \mathbb{Z}_N, \quad x \mapsto ax + k \mod N$$

over an n-letter alphabet is insecure because its key space is to small.

$a^{-1} \bmod N$ exists iff $\gcd(a, N) = 1$.

$\Phi(N)$ = number of integers in the range $1, 2, \ldots, N-1$ that are coprime to N.

So the number of enciphering keys (a, k) is only

$$\Phi(N) \times N$$

For $N = 26$, $\Phi(N) \times N = 12 \times 26$.

Computer Demo

An easy way to increase the size of the key space is to use a permutation cipher

$$f_E : \mathbb{Z}_N \to \mathbb{Z}_N$$

$$\{0,1,\cdots,N-1\} \xrightarrow{\cong} \{0,1,\cdots,N-1\}$$

There are $N!$ such permutations/enciphering keys

For $N = 26$, there are

$$26! \cong 2^{88}$$

keys.

But such a system can be broken using frequency analysis.

Computer Demo

Most frequent letters

plain	cipher
space	4
E	U
T, S, A	
S	~~E~~ or A
SC SASU… SC	AN

To counter frequency analysis a cryptosystem should not always encipher any given letter of plaintext as a single letter of ciphertext.

Vigenère cipher

Invented by Giovan Batista Belaso in 1533. Very popular in the 19th century, and misattributed to Blaise de Vigenère.

It is a "multiple Caeser cipher" with enciphering key any word you like in the alphabet.

For instance, over the 26-letter alphabet

A, B, ..., Z

we could choose

SESAME

as our enciphering key. We encipher as follows:

plain: THISISATESTMESSAGE

SESAMESESAMESESAME

cipher: LLASUWSXWSFQWWKASI