

Ceasar cipher is bad for 2 reasons:

1. Lock exchange problem

A and B have to agree on a secret key k , without sending it on the public channel

2. Key is crackable from the secret message

Ex: Frequency analysis

If the message is in English, the letter "e" appears more frequently than any other letter. The most frequent letter in \hat{M} should be e

$$x = 4 + k$$

\uparrow
E

$$k = x - 4 \pmod{26}$$

The RSA protocol

Safer protocol, which resolves these two problems

1. no need to exchange keys.

uses two keys:

- a public one (for encryption)
- a private key (for decryption)

Everyone can send messages to B, which B is the only one who can read them. (Can also be used the other way around, for certification of identity)

2. Secret key is not crackable in practice

To crack it, you need to factorize a very large number, and that's a NP-complete problem

