affine cipher

- Euclid algorithm for GCD
- → multiplicative cipher - problem: A B always A. 0 13 26
- → affine cipher = mult. + caesar ciphers

cipher: plain txt ⟶ multiply → mod key
by key A

→ challenge: key 8: → many keys result in the same sequence, some repetitive keys
~8-9 million keys.

solve this problem:

↳ diff. letters → same letters

↳ we can't decrypt it back

↳ solution: GCD(keyA, 26) == 1

if key is not relatively prime ⇒ key not working for us

$$\frac{\#\text{ of symbols in the alphabet}}{\#\text{ of symbols we accept for our cipher}}$$

multi. cipher:

+ we need inverse modulus algorithm

encryption method/func.

user: enters message + key only

$= 2023$

* key split method:

keyA = 2023 / len(msg)

keyB = 2023 % len(msg)

decryption: coming soon...

→ challenging, complex.