#flo #inclass #intersession

1 | Crypto (graphy)

oldest version: caesar cipher!

plain text: cryptography is fun encryption: pick a number S, and shift every number forward by S (w/ wrap) cipher text: Hwduytlwfumd nx kzs

not hard to recover the org message! brute force message -> 25 options also, not likely to have multiple values of S that would output english

1.1 | the cast.

these are the terms we use to descibe scenarios

protagonisnts **Alice** the one who sends messages **Bob** the intended recipient

antagonisnts **Eve** the eavsdropper (badum-tschh). this is the important view to consider!

1.2 | substitution cipher

the alphabet: `abcdefghijklmnopqrstuvwxyz` do ”pairwise matching” #review legit just get them together

any extra struture constrains the search space, makes it easier to crack

1.3 | bad encryption

T PXVW X QNIOD CXNVWDEIK RWCEAKRNXRTEA EF QPTK UNEUEKTQTEA

T, X, EF

most common: E

t, a, o, d, and w. **e, s, d, and t** both: D, T

A ends two words -> t, a, o, d, w tea -> ing t, i e, n a, g

QED f -> o

tea -> ate: ta, et, ae

t -> i x -> a ***** giveaway: spaces. segmenting words -> easy to break! could use space as another letter to alphabet, but that is easy to crack. instead, let’s just rm the space altogether!

practically unbreakble, unless you have a long cipher! then, we can use freqnecy of letters. ofc, we need a size that is big enough to be around representative of our ideal freqnecies.

1.4 | modular arithmetic

> A and B are congruent mod n if their difference is a multiple of N

and with the mod func, we can do arithmetic!

- add, subtract, multiply,
- exponentiation but you cant just reduce it
  - Fermat's little theorem
    - if A is an int, then A^{P} is congruent A mod P if A != 0, then A^{P-1} = 1 mod p

```
title: totient
totient (plural totients) (mathematics) **The number of positive integers not greater than a specified
```

but we care about euler's totient theorem: if $gdc(a, n) = 1$, then $a^{\phi(n)} \equiv \quad \mod n$