Lecture 1 §1.1 2022/3/28

Prereqs

- Linear algebra (upper div)
- Basic proofs

Not Prereqs

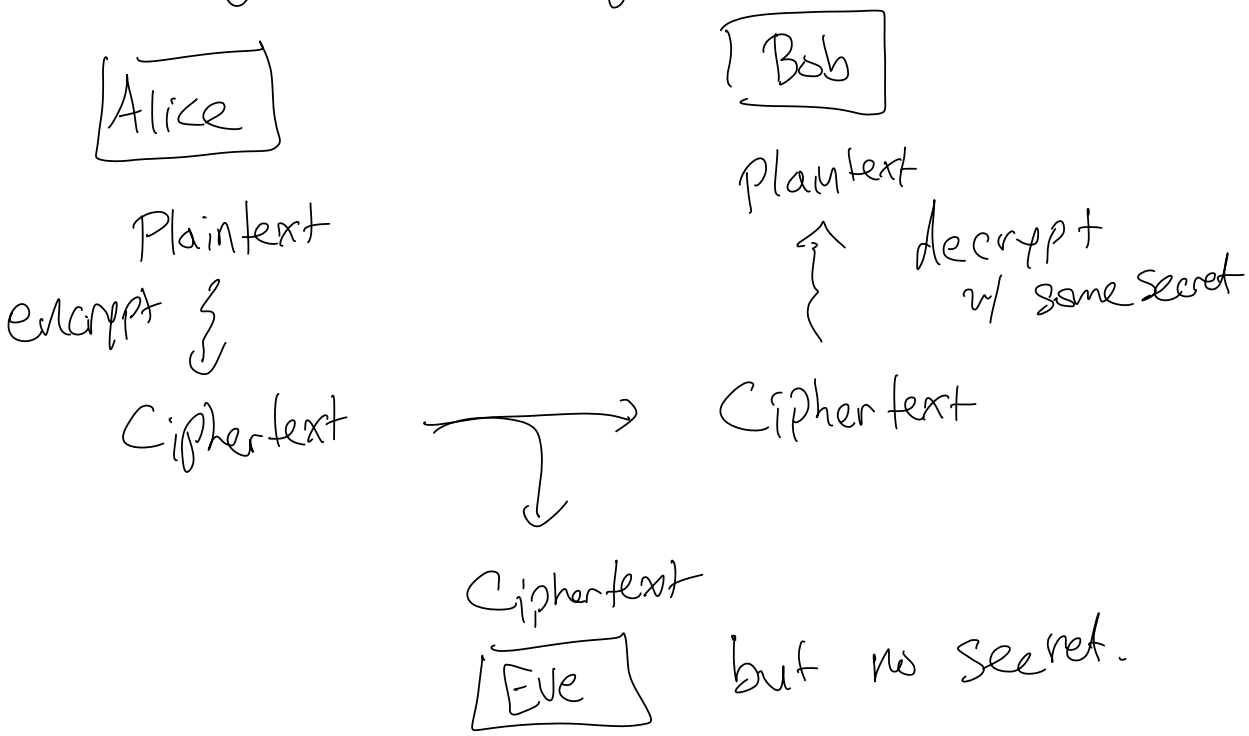
- Abstract algebra
- Programming

Cryptography is the construction & analysis of protocols that allow private communication over public channels.

From Greek: kryptos (secret) + graphen (writing).

First used by Poe!

A diagram of a generic crypto system.



A crypto system is the method to encrypt / decrypt a message combined w/ some extra key.

The security of the system depends on the secrecy of the key but not on the secrecy of the system itself.

Cryptanalysis is the process of trying to break a cryptosystem.

So Eve performs cryptanalysis to try to learn what Alice sent to Bob.

Ex 1 Shift Cipher / Caeser Cipher.

plaintext abcde ... wxyz
↓ ↓
CIPHERTEXT DEFGH ... ZABC

shift by 3 the key.

hello Decrypt by shifting back.
↓
KHOOR

Cryptanalysis Only 26 possible keys.

Just try them all.

	A F Y R F Y K	
1	b g z s g z l	✗
2	c h a t h a m	✓
3	d i b u i b n	✗

Convention plaintext written lowercase
CIPHERTEXT uppercase.

Any cryptosystem w/ a small key set is vulnerable to brute force analysis.

Ex 2 Substitution Cipher

plaintext
↓
CIPHERTEXT

a	b	c	d	e	—	bcd
↓	↓	↓	↓	↓		↓
C	Z	E	D	X	—	ZED

Each letter appears once. The key is the table.

Cryptanalysis See book, wikipedia, etc but key idea is analyze letter frequencies:
e appears most often, then t, a, ---
most common digraphs are th, he.

Ex3 Vigenere Cipher

The simplest polyalphabetic substitution cipher.

(Most classical cryptosystems are polyalphabetic substitution ciphers)

plaintext → CIPHERTEXT

hello → JJPNT

key: bed
234

bedbe
23423

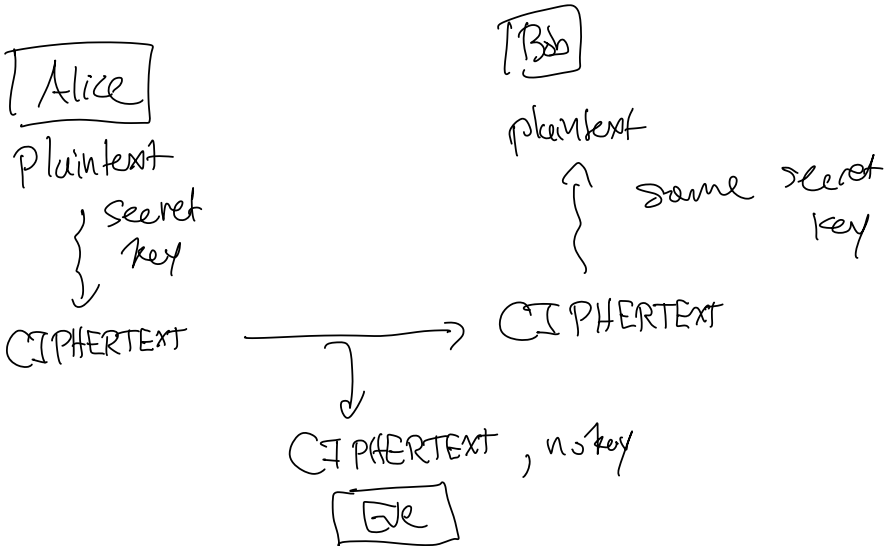
Repeat key & shift each letter of message by a different amount.

To analyze, first look for key length, then analyze like simple substitution cipher w/ statistics.

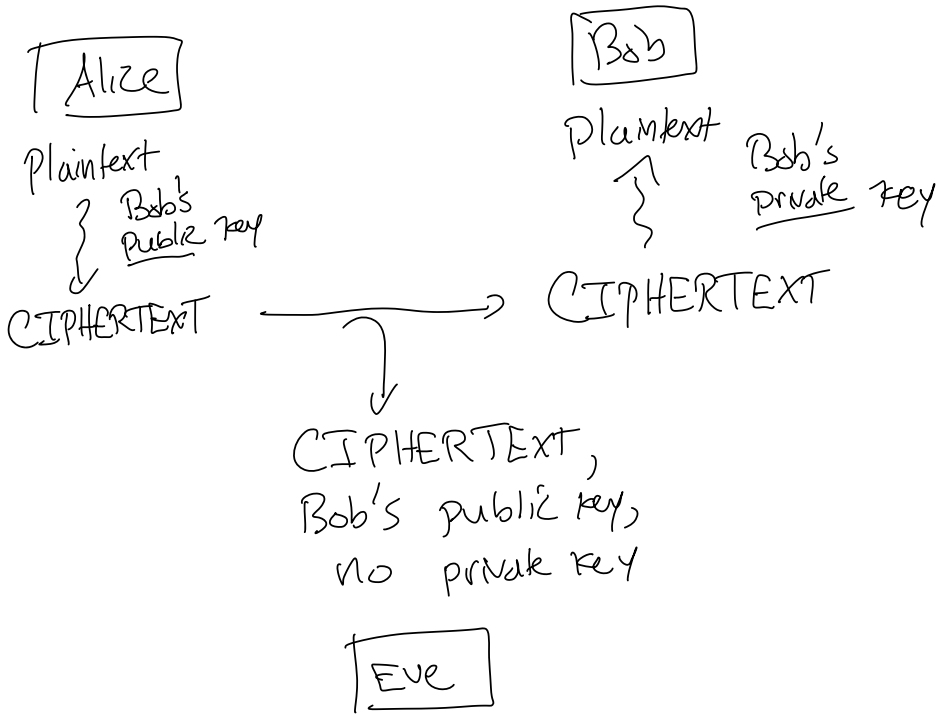
See wikipedia which has a very thorough description.

Symmetric & Asymmetric Ciphers

Symmetric cryptosystem:



Asymmetric cryptosystem:



Symmetric

- Alice & Bob need a shared secret (hard to arrange?)
- Designed w/ ad hoc mixing operations
- Fast
- ancient

Asymmetric

- No need for shared secret ~ convenient
- Related to math problems thought to be hard
- Slow
- Recent (<50 years old)