1. Classification of Cryptography
2. Basics about Cryptographic setups
3. Substitution cipher
4. Attacks

1. classification:

Modern applications of Cryptography?

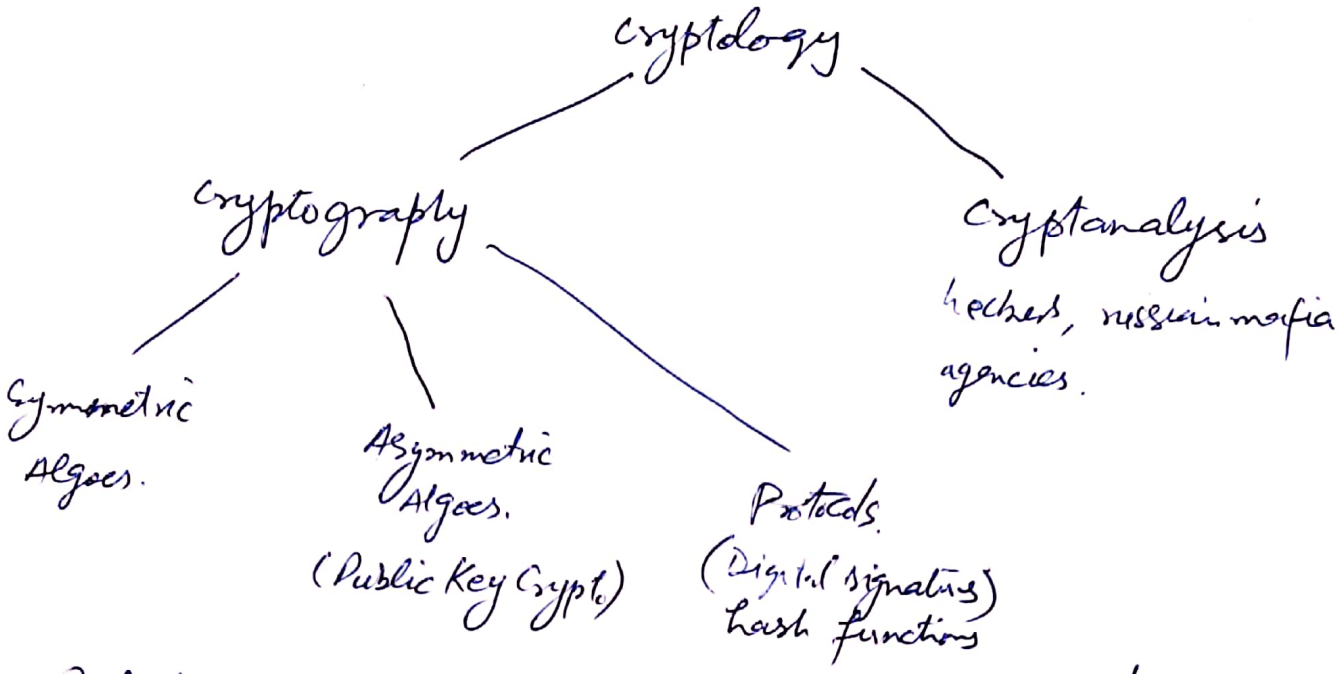
- installed & PC
  - GNU GPG
  - TrueCrypt
  - Secure Shell (remote file transfer)
  - (Plug-in) for Thunderbird
  - S/MIME email encryption
- network centric
  - cell phone (GSM cell phones)
  - hdcp multimedia port
  - bank cards
  - VPN
  - ~~EPS~~ e Passport
  - electronic citizen cards
  - On line banking

Crypto on board

- i-Pod
- Kindle

Consumer products

Business + Crypto



Relationship of Crypto & Security.

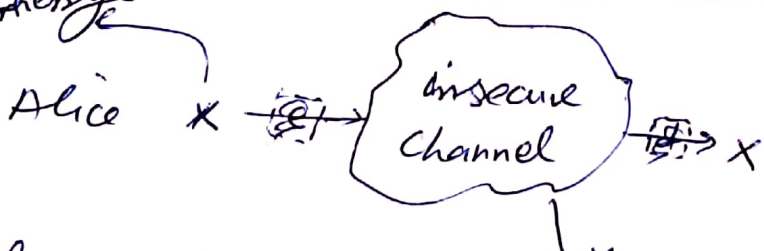
Crypto is one part of Security

So for security you'll have to do more than Crypto.

2. Set-up for Symmetric cryptography

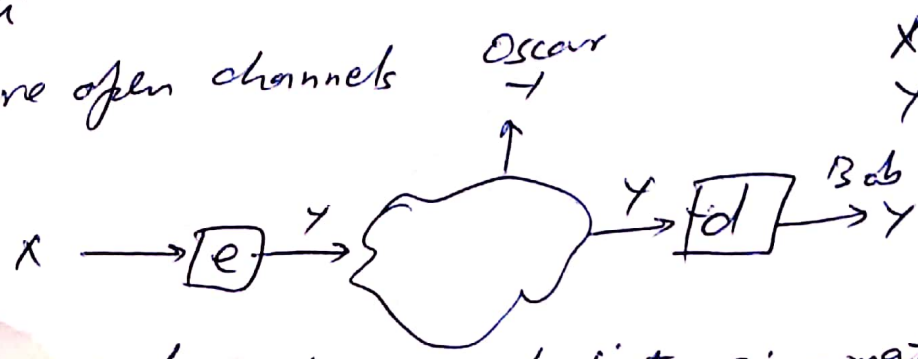
Ex: Communication over insecure channel.

email message



channel examples: internet, air waves GSM, wifi

These are open channels



x is plaintext

y is cipher text.

y is random stream of bits, e is a mathematical formula turns x to y.

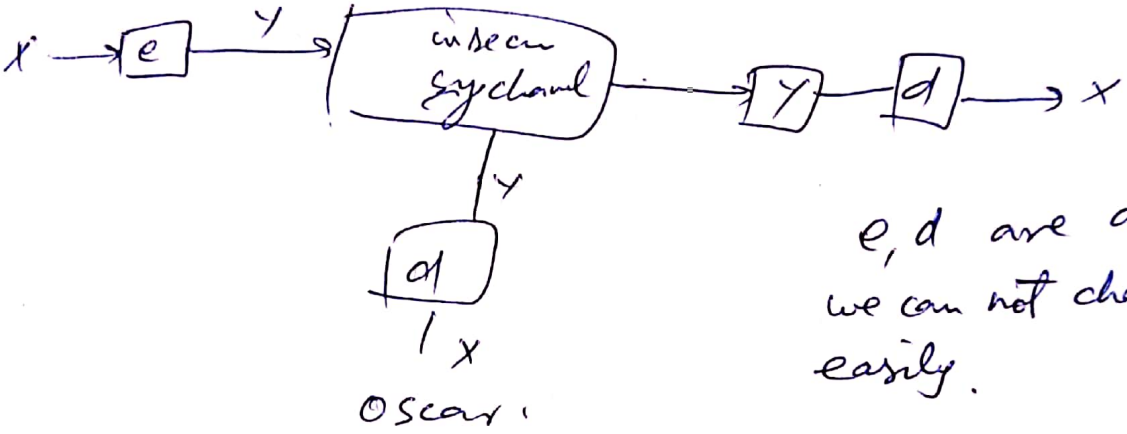
e & d functions are kept secret. (2)

crypto started 2000 BC and till 50 years ago, people thought e & d to be kept secret.

probably every algo is breakable

but we think algo is broken in large time, then secure.

In practice: Never use an untested crypt algo



e, d are algos we can not change them easily.

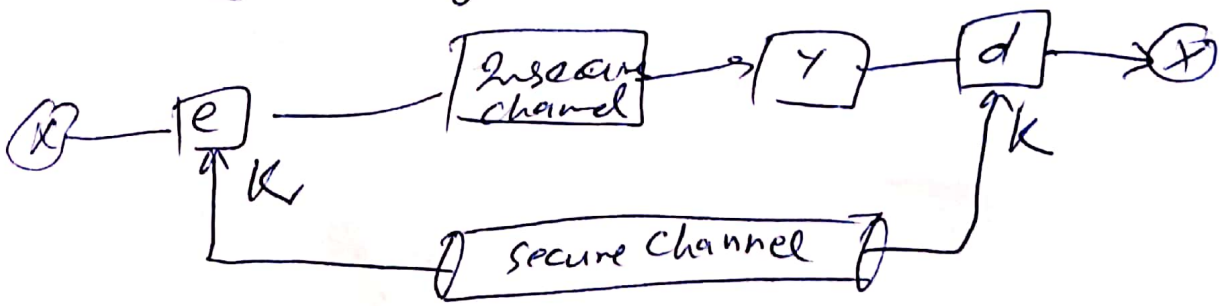
So ~~the~~ we use key (K)

simplest ways to break a system is Brute force. (use all possibilities of key).

K ≙ key, $|K| = \mathcal{K}$ ≙ key space.

= # of keys.

* Now key must be shared personally before communication (or through a secure channel).



Kerckhoffs' Principle [1883]

"A cryptosystem should be secured even if the attacker knows all the details about the system, with the exception of the secret key."

Remark: Kerckhoffs's principle is counter intuitive.

[Normal thinking keep e, d secret so no need of this principle]

3. Substitution Cipher (an example of crypto. system)

- historical ciphers (stupid now)
- Ciphers operated on letters (not bits/bytes)
  (40 to 50 years ago)
- Idea: replace every plaintext letters by fixed ciphertext letter.

  Ex: A → l, B → d, C → w, ...

  e.g., ABBA → lddl

  Q: Is cipher secure? NO.

  ?: How can we attack the cipher
  (attempt all keys)

  1st Attack: Brute-Force or exhaustive key search.

  Q: How many keys?

  $26 \cdot 25 \cdot 24 \cdots 1 = 26! \approx 2^{88} = 2^{56} \cdot \underbrace{2^{32}}_{10^9}$

  so if a machine can do 2^{56} in one day

  10^9 days are required.

  ⇒ key space is too large.

  So this attack does not work.

2nd attack: (stupid

letters are not equally likely.

frequency of plaintext letters is preserved.

e.g.: e is the most common, (13%)
t is the next common (9%)

So do letter frequency analysis

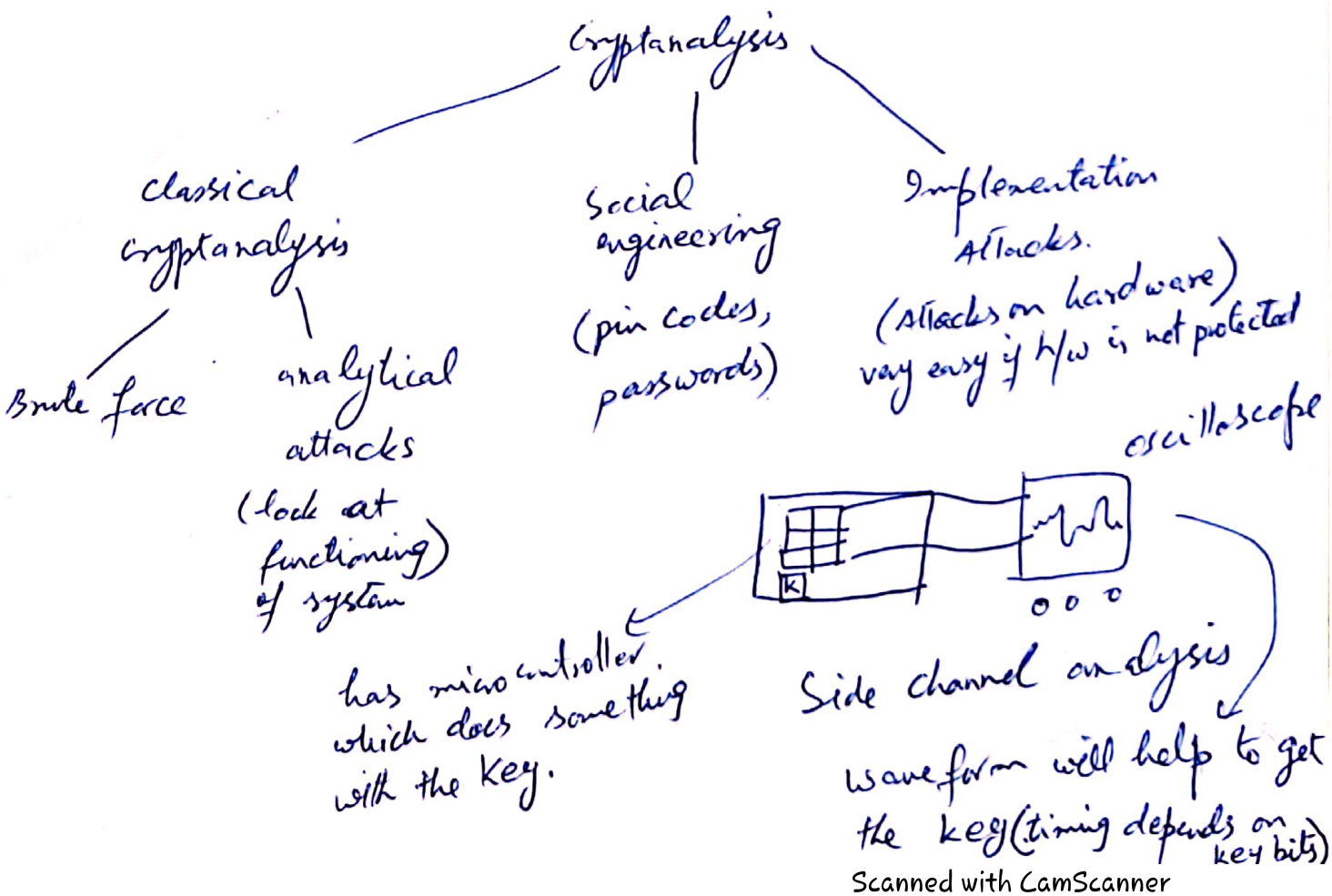
if Q in the has heighest frequency, then it is E.

Homework: Try it.

This works b/c identical plaintexts maps to identical cipher text symbols.

4. Classification of Attacks

There are often many possible attacks approaches ("Attack vectors")



Textbook: A course in Number Theory and Cryptography

by Neal Koblitz

- Elementary Number Theory.
- Finite field & Quadratic Residues.
- Cryptography (Simple systems, Enciphering Matrices.
- Public key (RSA, Discrete log, Knapsack zero knowledge protocols and oblivious transfer).
- Primality and factoring
- Elliptic curves.