

CISS 451

CRYPTO & COMP SECURITY



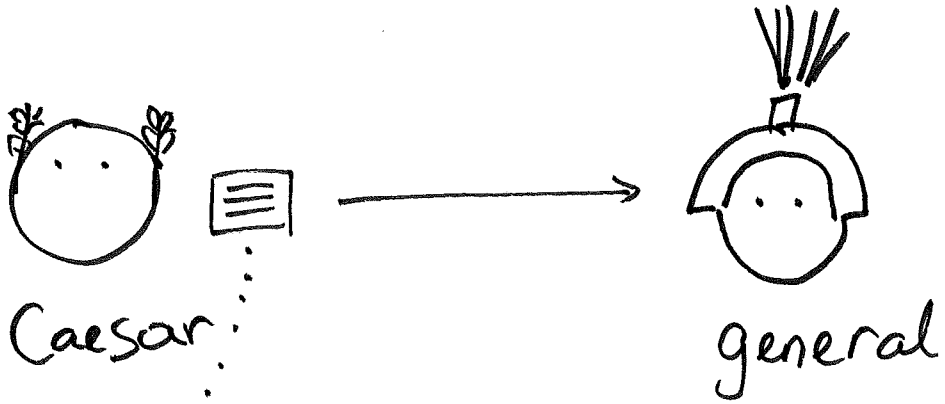
Y. Liow

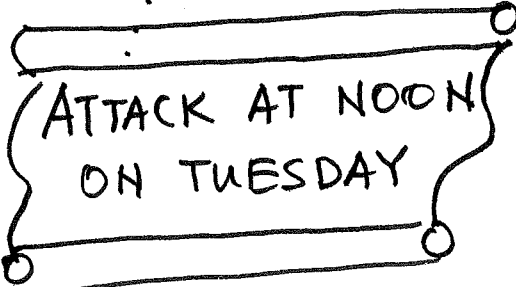
OVERVIEW

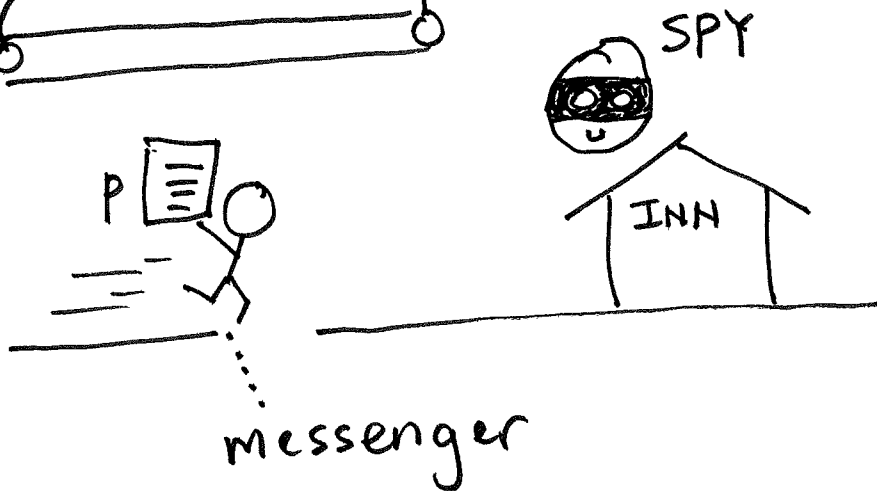
CAESAR

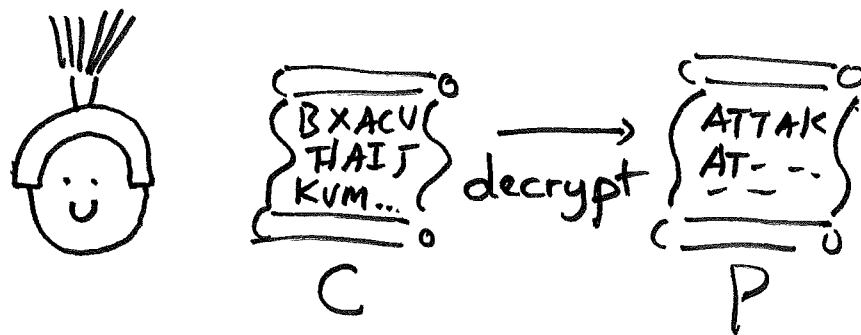
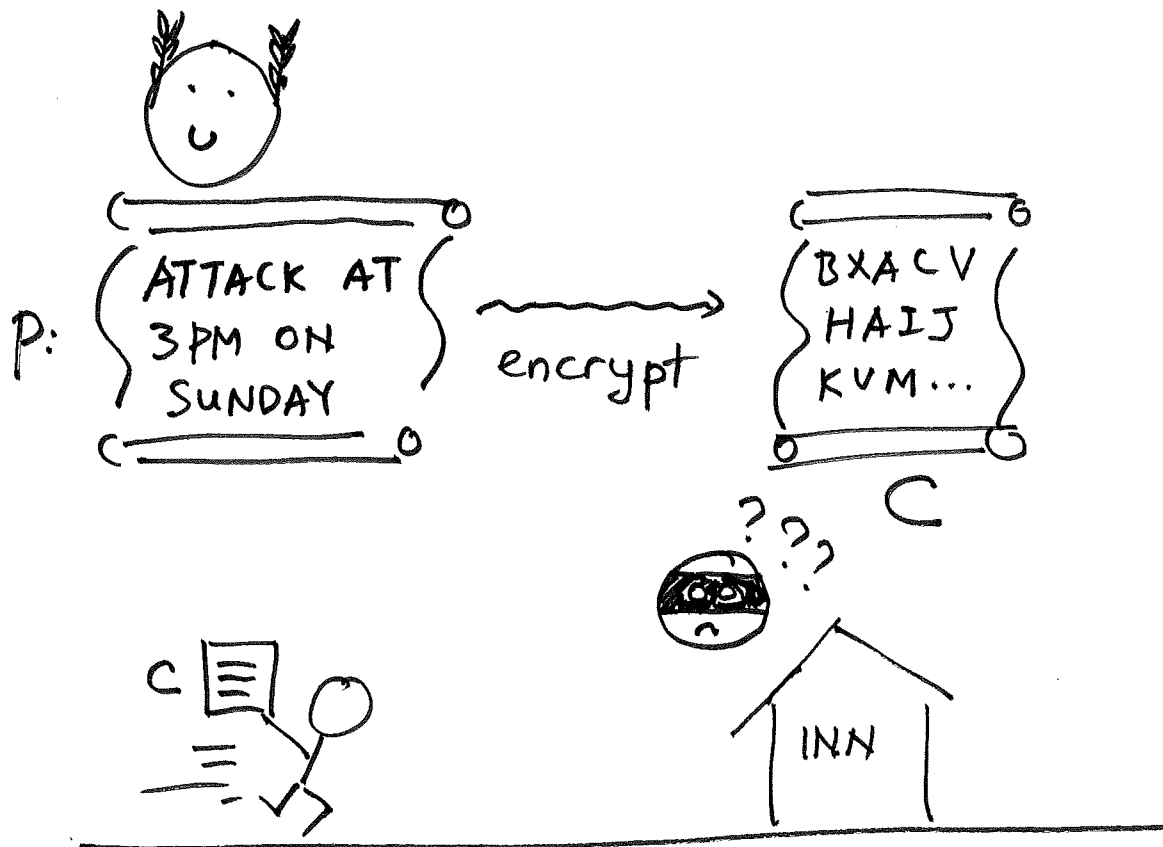
CIPHER

... an example



P:  A hand-drawn scroll with a wavy border. Inside the scroll, the text "ATTACK AT NOON ON TUESDAY" is written in capital letters. To the left of the scroll is the letter "P:".





How?
Caesar cipher ...

Caesar cipher



α β γ δ ... } encrypt
 \downarrow
 δ

α β γ δ ... } decrypt
 \uparrow
 δ

or (English)

a	b	c	d	e	...	w	x	y	z
\downarrow	\downarrow	\downarrow	\downarrow	\downarrow		\downarrow	\downarrow	\downarrow	\downarrow
d	e	f	g	h		z	a	b	c

(For English, remove spaces, punctuations and use only lowercase or only uppercase)

$$a \rightarrow b \rightarrow c \rightarrow d \equiv a \rightarrow d$$

Can think of this as a

"shift forward by 3"
backward

encryption

decryption

caesar
cipher

\equiv

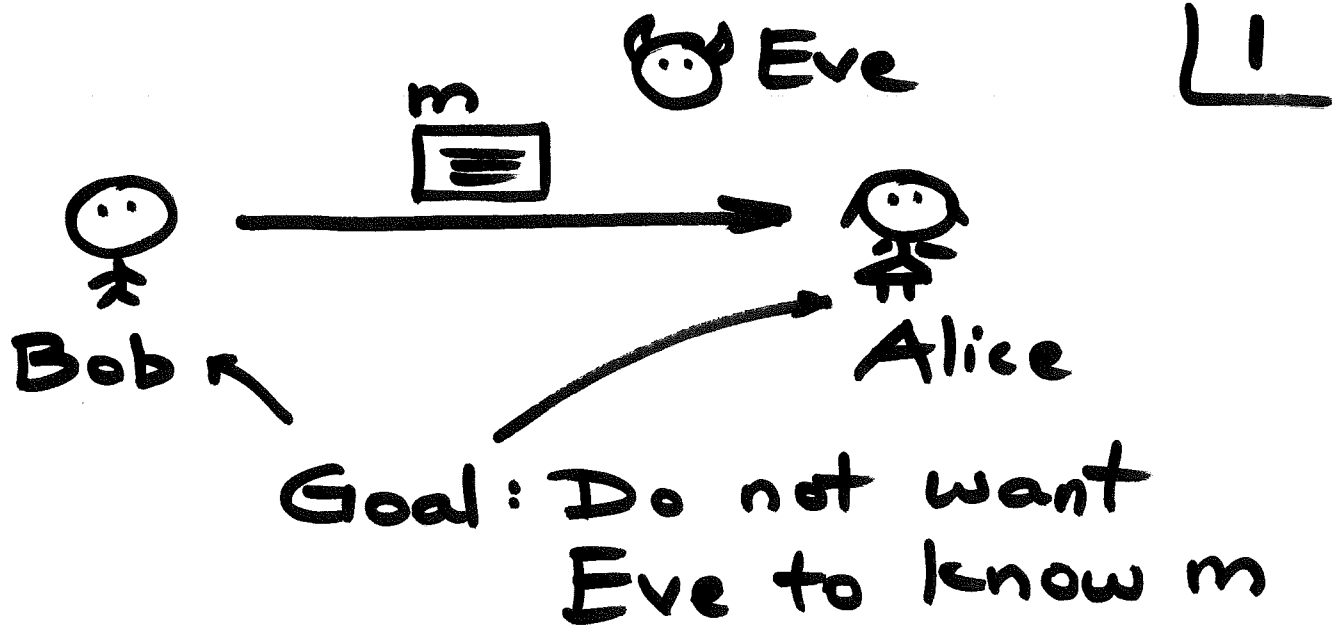
Shift cipher
with key = 3

Modern
terminology

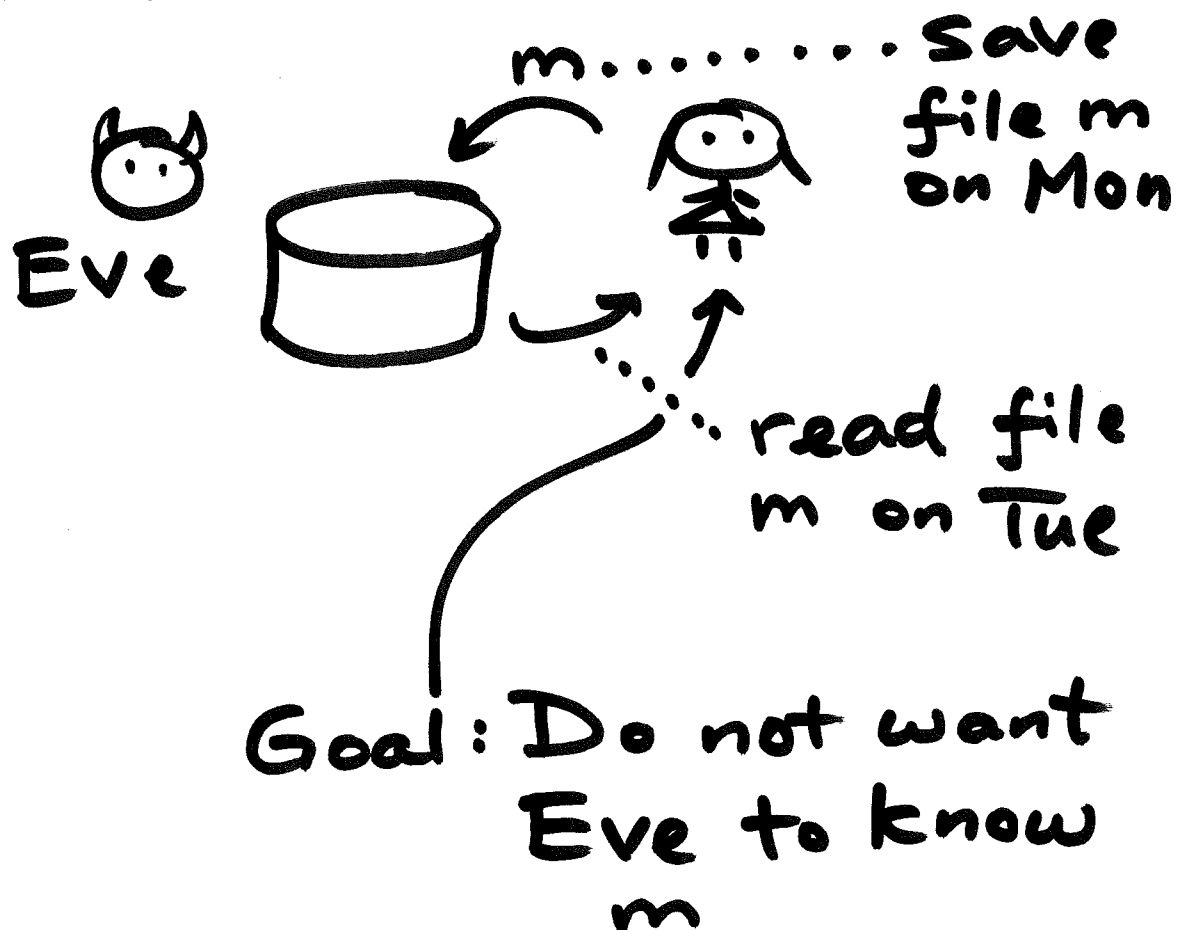
Caesar never
thought about
changing 3

to something else

... enemies not smart
anyway



Not just communication.



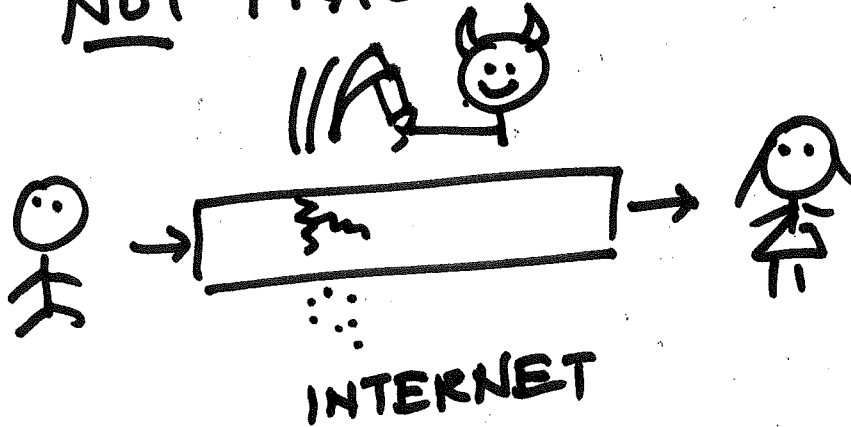
Eve



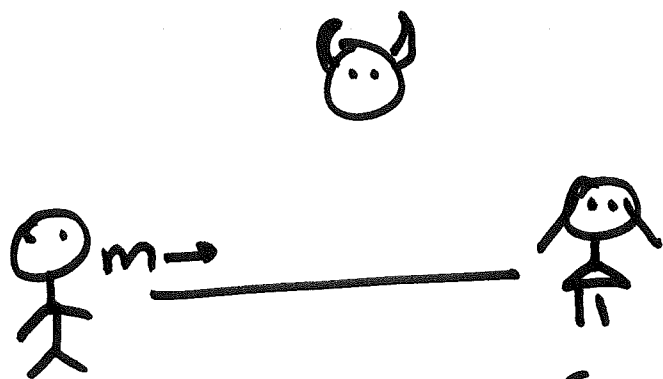
Secure channel

i.e. Eve cannot read contents traveling in secure channel

NOT PRACTICAL



WIRELESS +
INTERNET etc .
— PUBLIC



CONFIDENTIALITY

- Eve can't read m

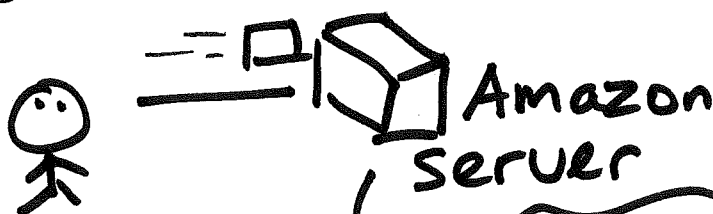
Anything else?



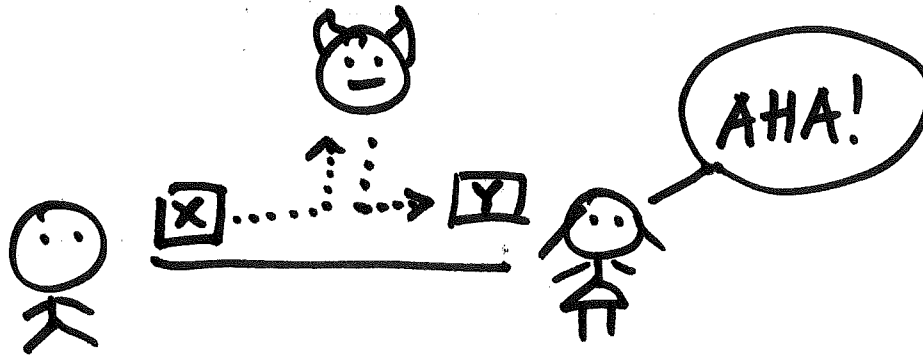
AUTHENTICATION

- m comes from Bob

Not just communication



Did Bob make that purchase?



INTEGRITY:
 m was not
 altered
 during transmis-
 sion



NONREPUDIATION:
 Bob can't say
 "I'm not the
 sender!"

AUTHENTICATION \neq NONREPUDIATION
 Why? Alice might have created
 m

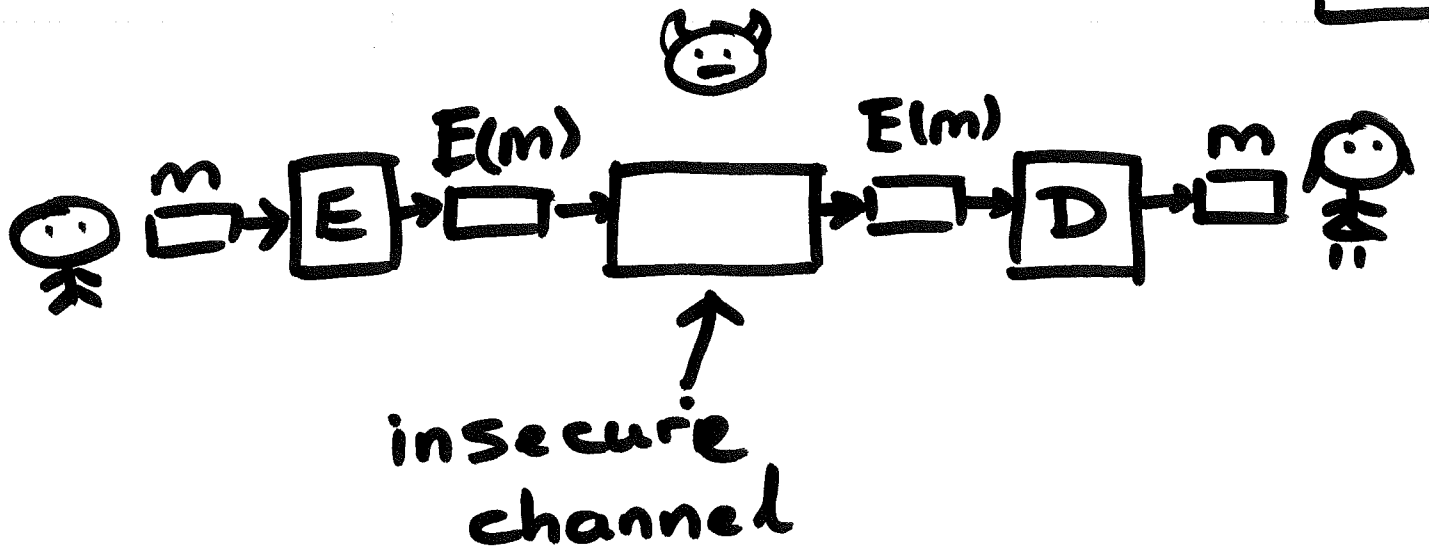
Stick figure \equiv Devil

Confidentiality
 authentication
 integrity
 nonrepudiation

LOTS OF
 GOALS...
 ☹

CRYPTOGRAPHY!

☺

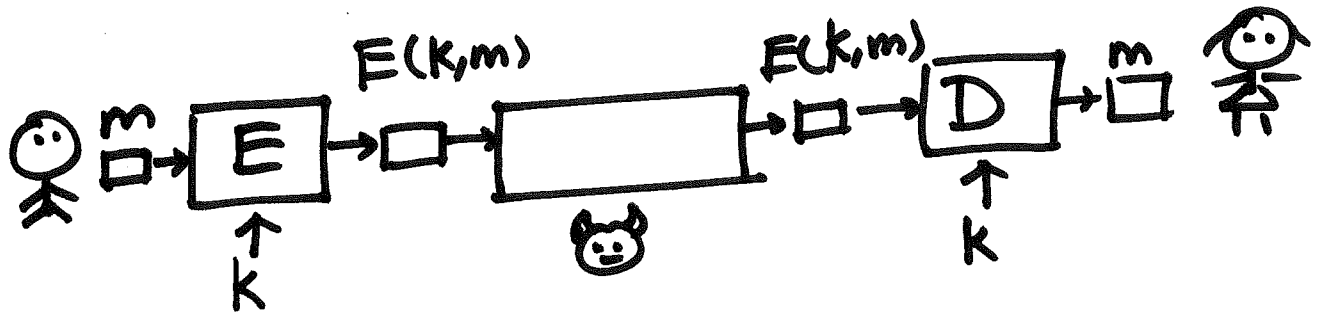


$$D(E(m)) = m$$

E - encryption function
 D - decryption function

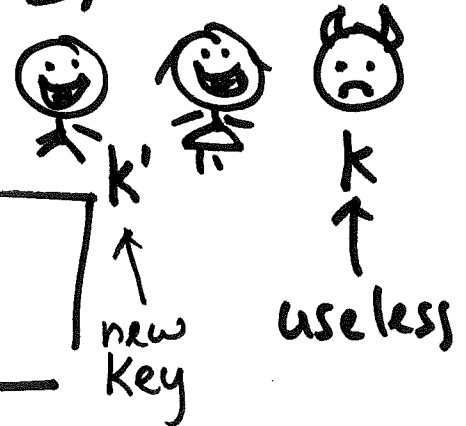
However... want E and D
be configurable with an
extra piece of data — key

7



Why? If Eve captured the
engineer who built the E, D
machines ... change k.

$$D(k, E(k, m)) = m$$



Here assume

encryption key

= decryption key

E, D — the algorithm pair
is called the cipher

k — key

The possible values of k is
the set called key space — K

M — message space
the values you can
put into E

C — ciphertext space
the outputs of E

E, D, K, M, C

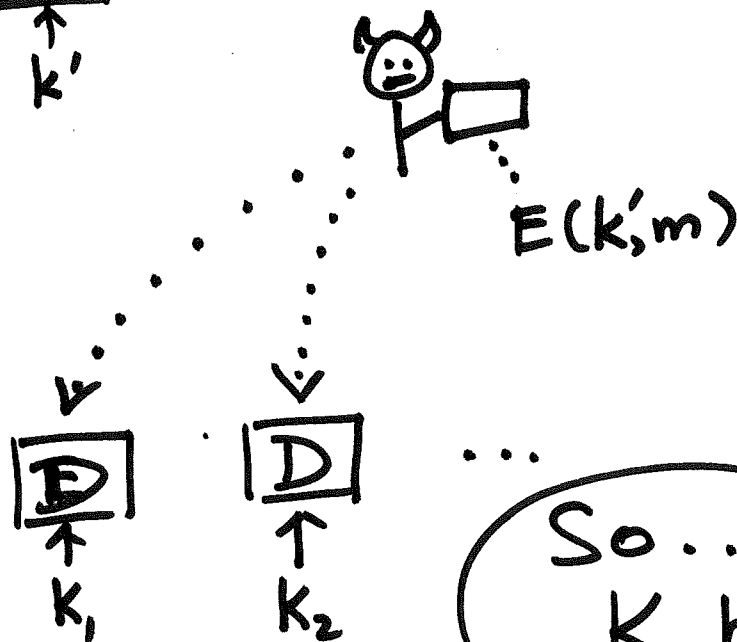
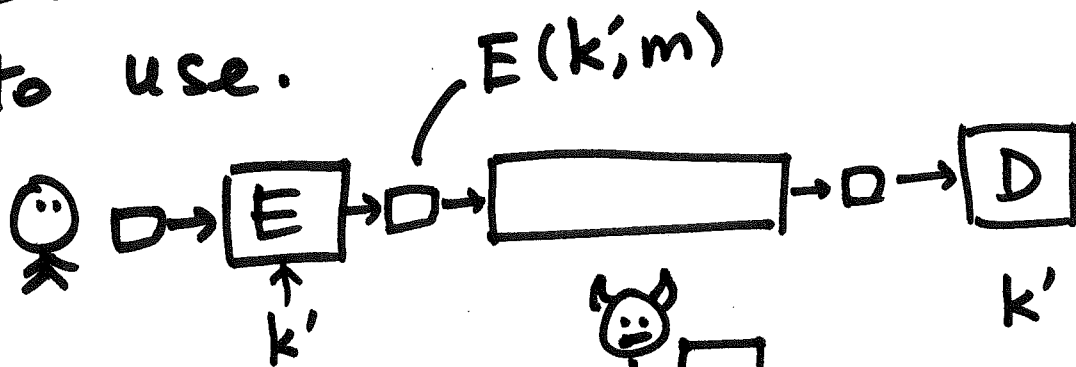
If Eve captured the
 engineer of E,D and
 tortured him/her to reveal
 algorithms

What will she do?



Bob and Alice
 change key k to k'
 and start using k' .

Eve doesn't know which key
 to use.



Try all keys.

So...
 K big!

Kerckhoff's Princ

Do not use "security by obscurity" ... reveal the algorithm E, D but make E, D run with keys.



By revealing E, D alg you can ask cryptanalysts to study the strength of E, D.

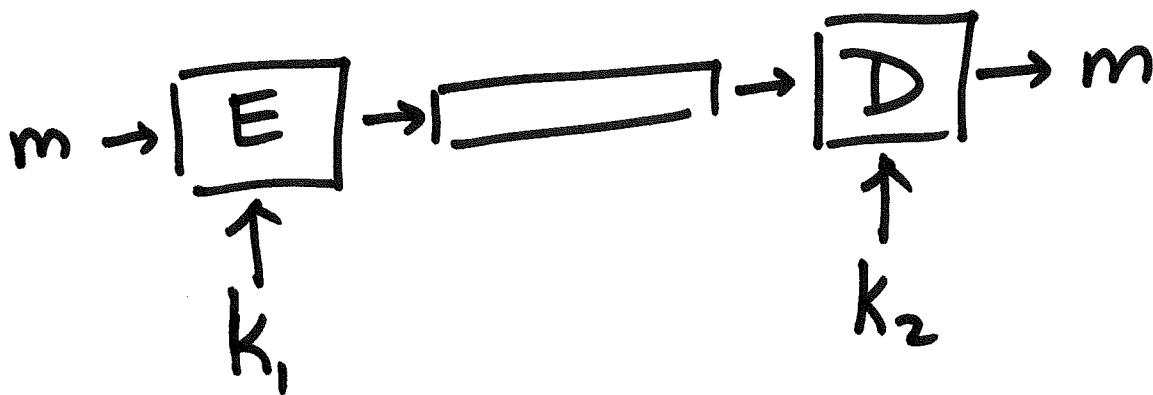
All modern + strong ciphers are public-reviewed.

Symmetric key cipher

Encryption key
= Decryption key

Asymmetric key cipher

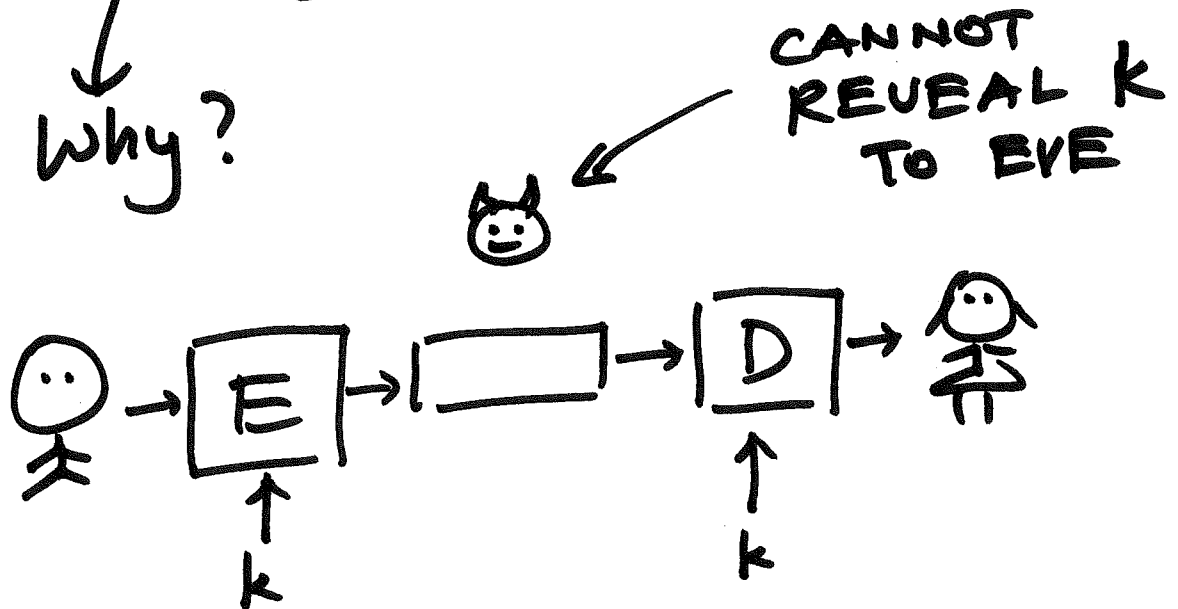
Encryption key
≠ Decryption key



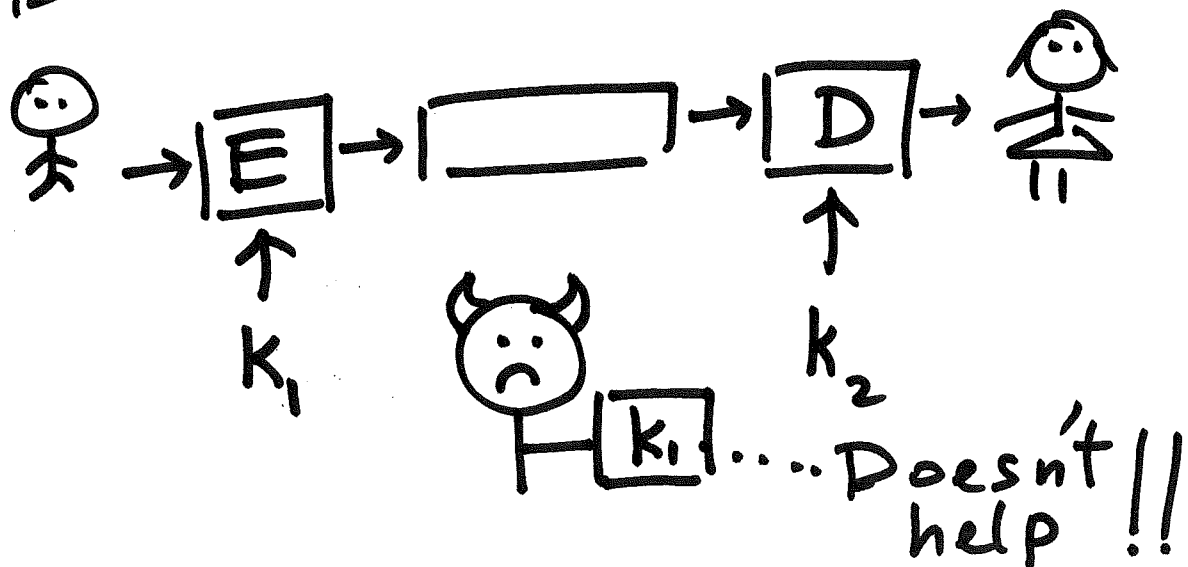
Asymmetric — VERY RECENT DISCOVERY 1970's !!!
(
 public key
 crypto

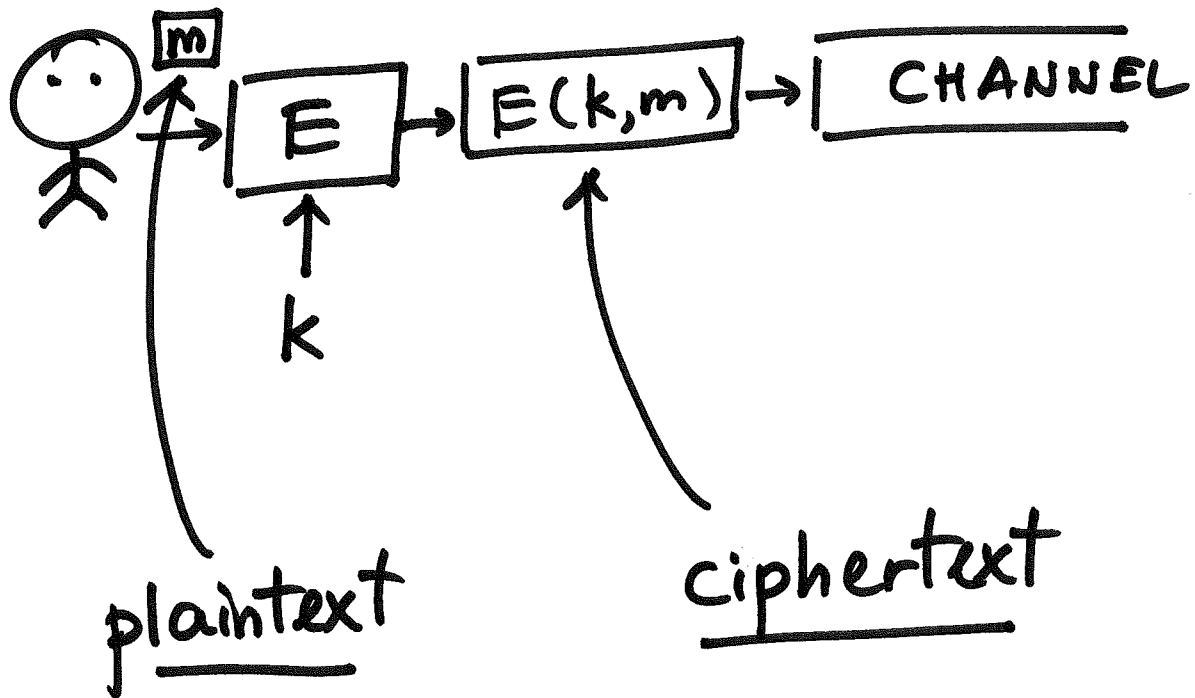
Symmetric - VERY OLD 12
BUT STILL
IN USE

Private
Key cipher
Why?



BUT FOR ASYMMETRIC ...





Cryptography - art + science
of keeping
msg secure

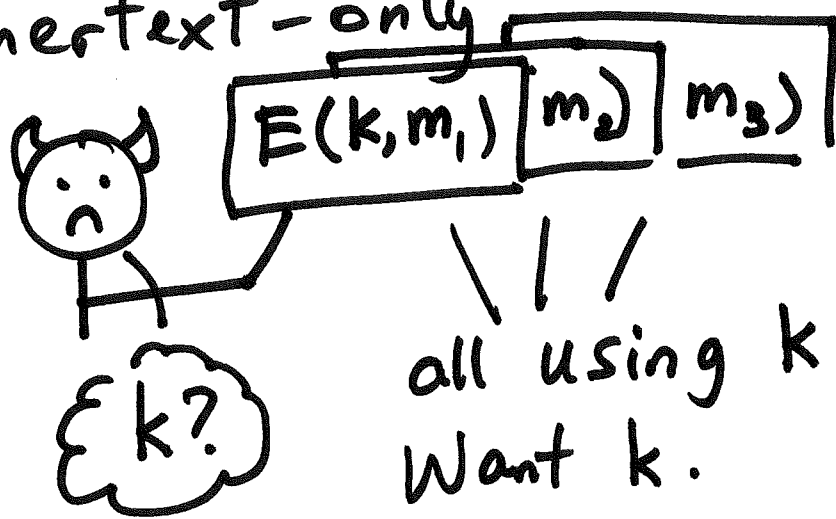
Cryptanalysis - study of
breaking
ciphertexts

cryptology - math aspects
of cryptography
+ cryptanalysis.

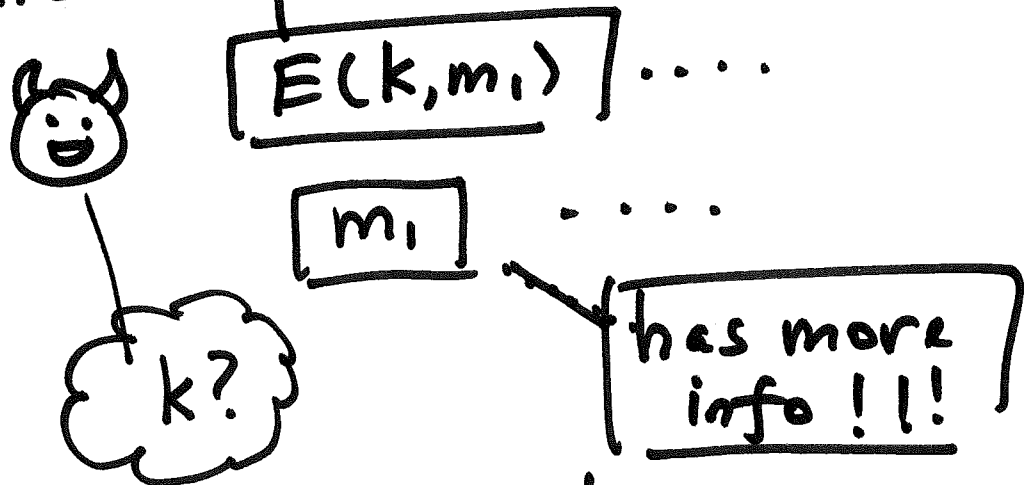
Eve's attack modes

14

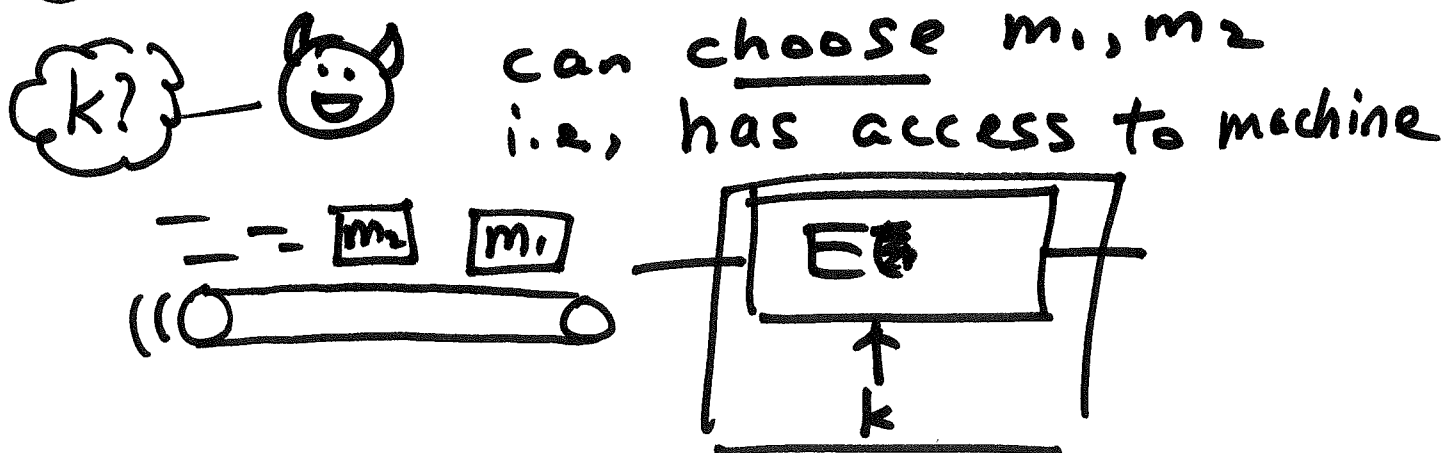
① Ciphertext-only



② Known-plaintext



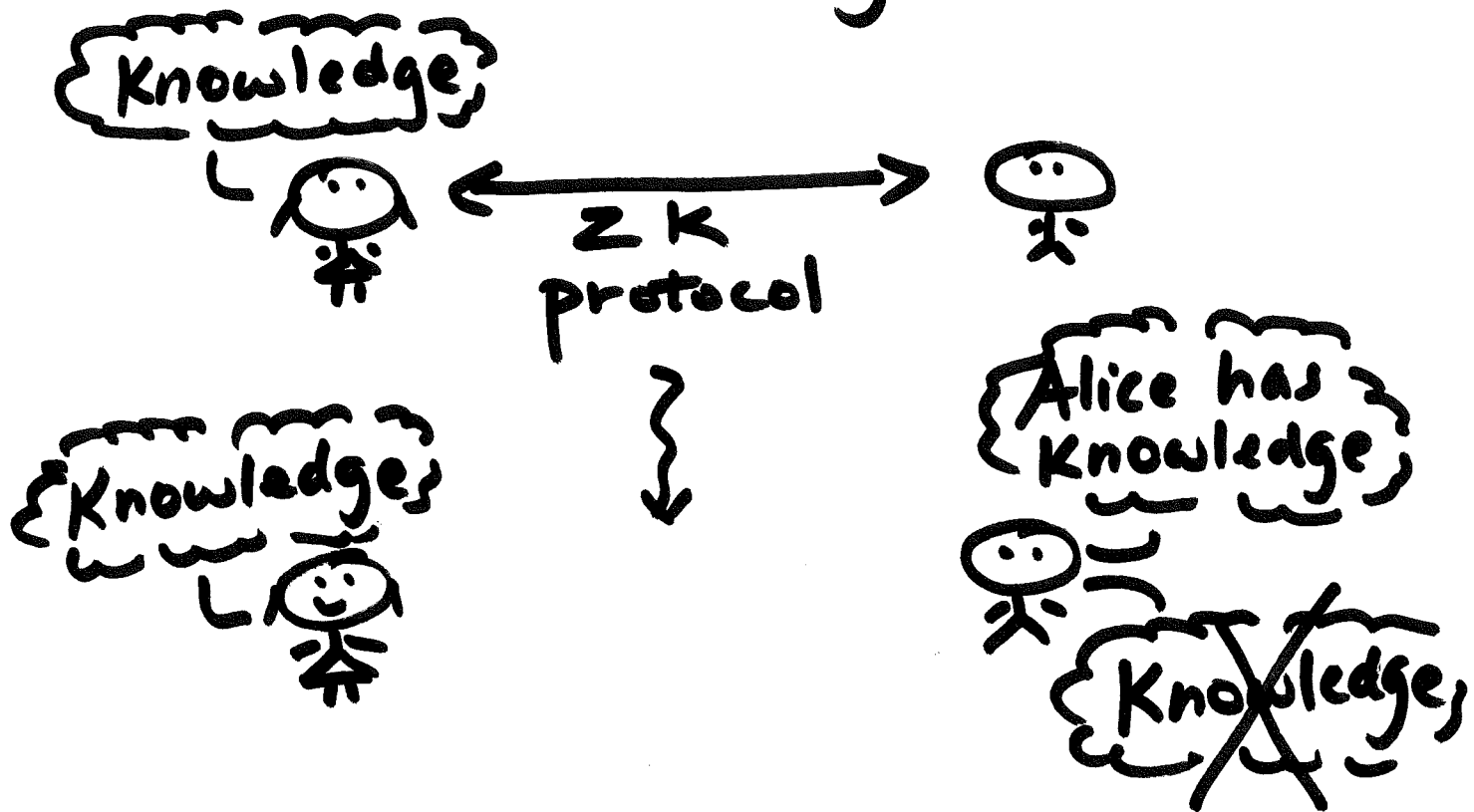
③ Chosen-plaintext



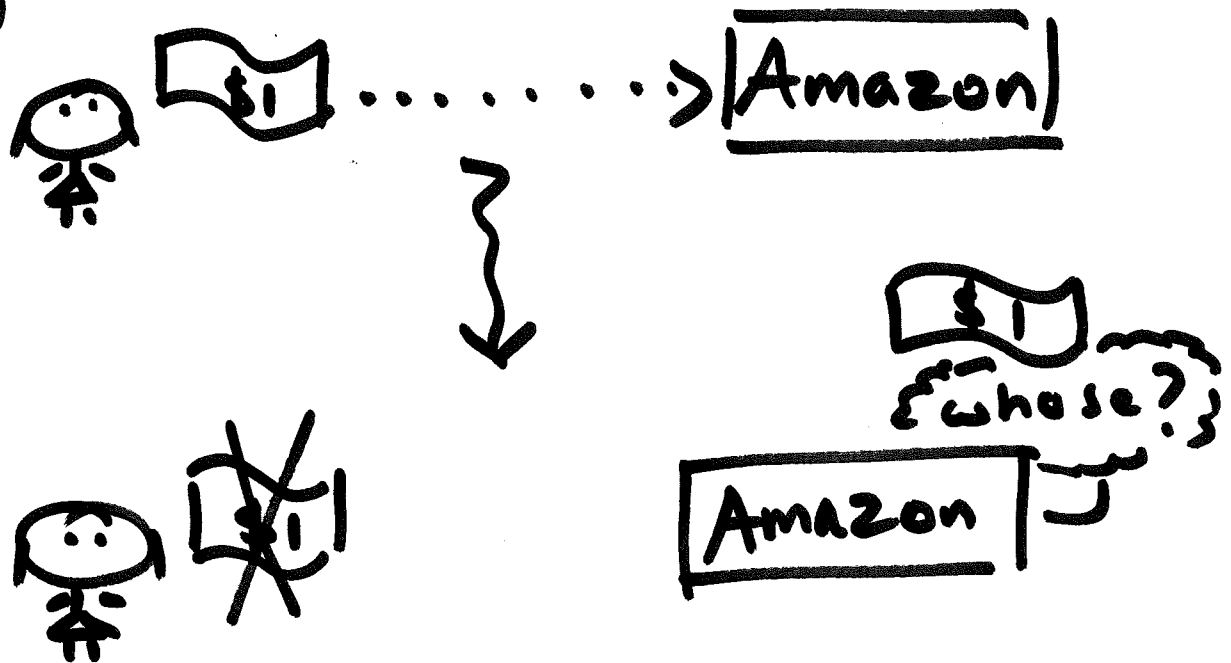
Of course for asymmetric
cipher Eve wants
decryption key to decrypt.

If she wants to
masquerade as Bob,
she also need encryption
key.

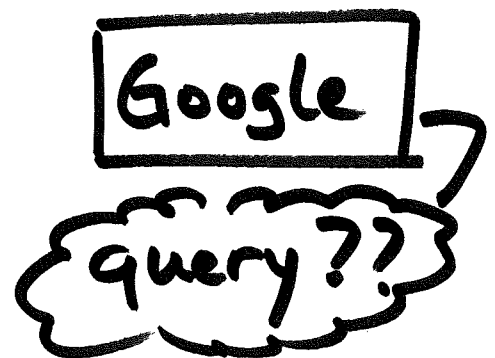
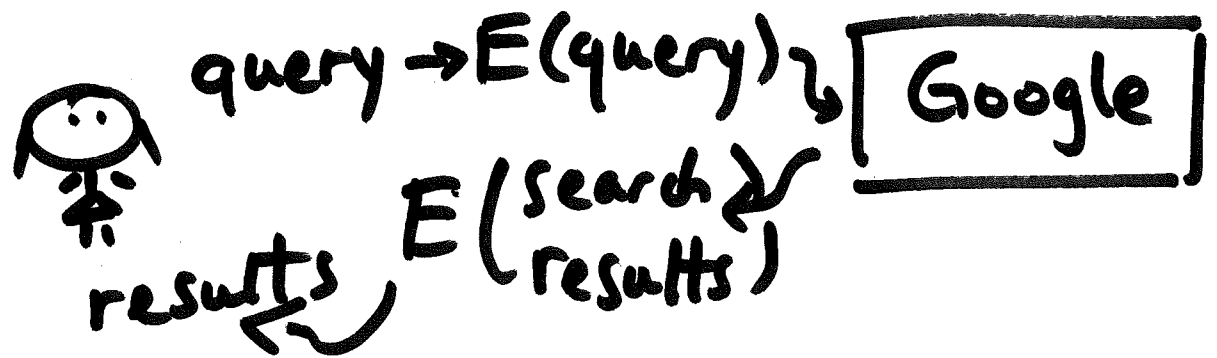
Zero knowledge



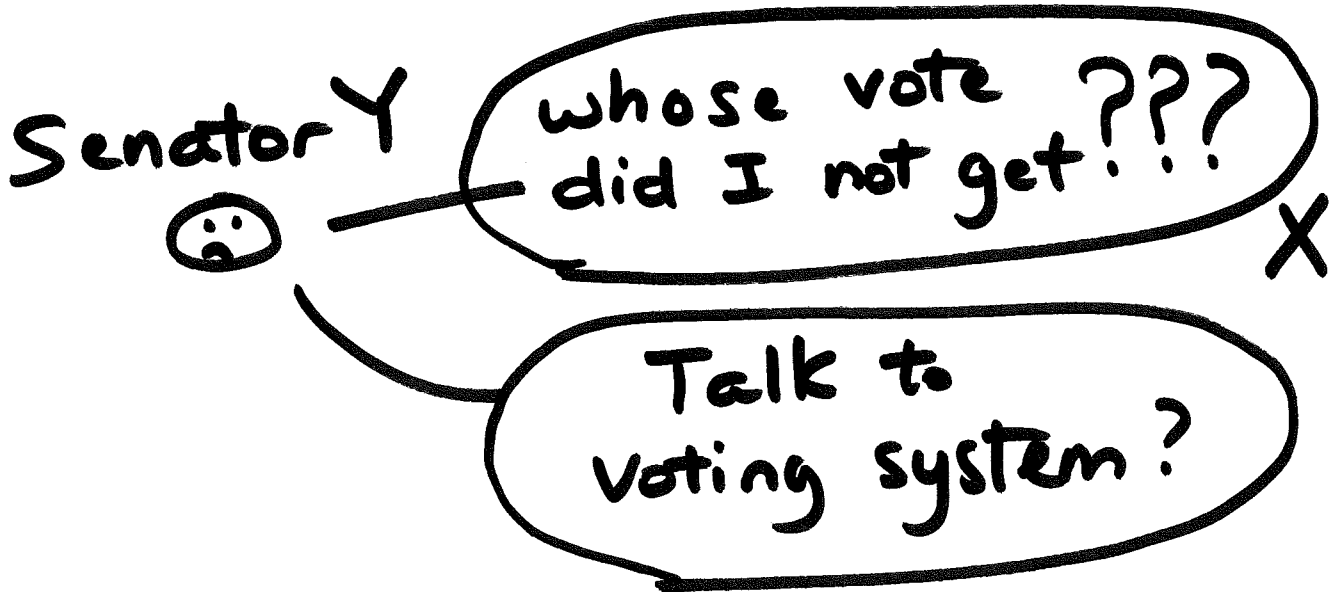
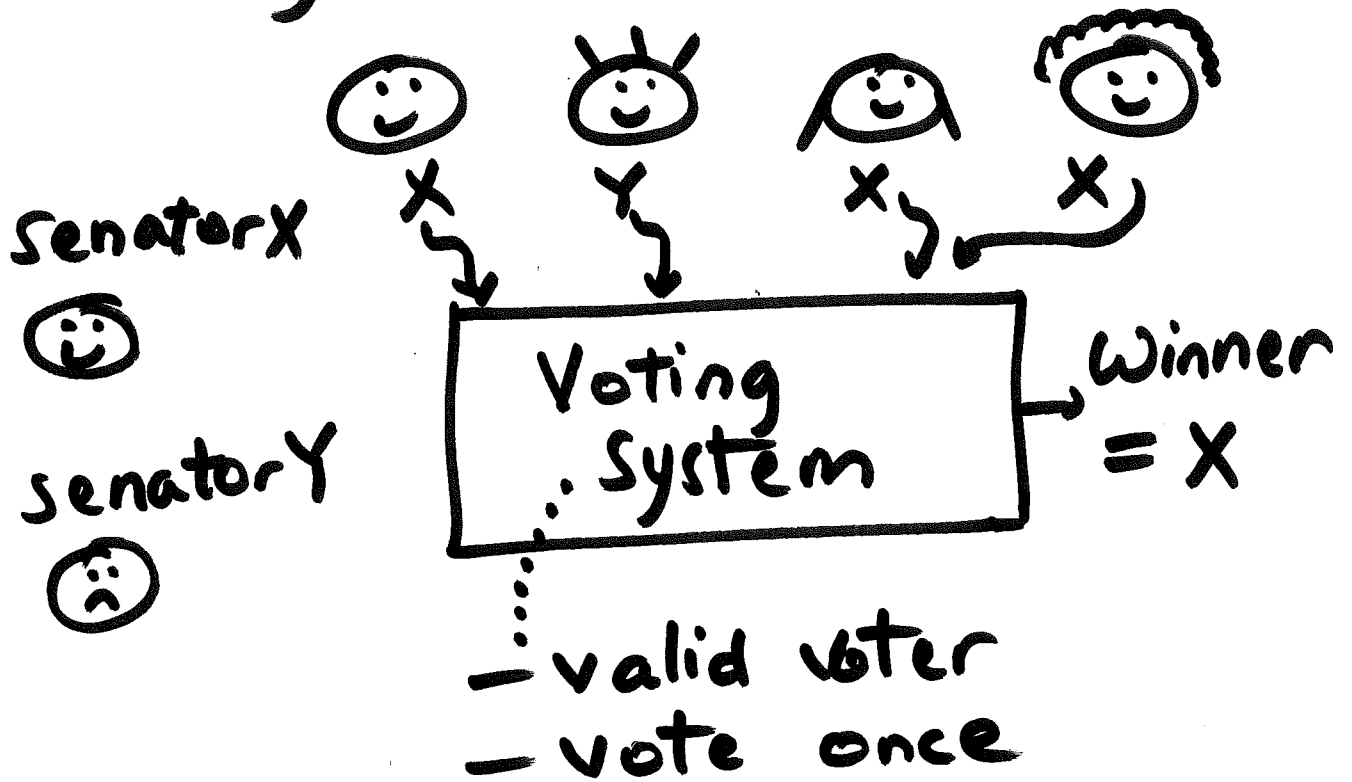
Digital cash



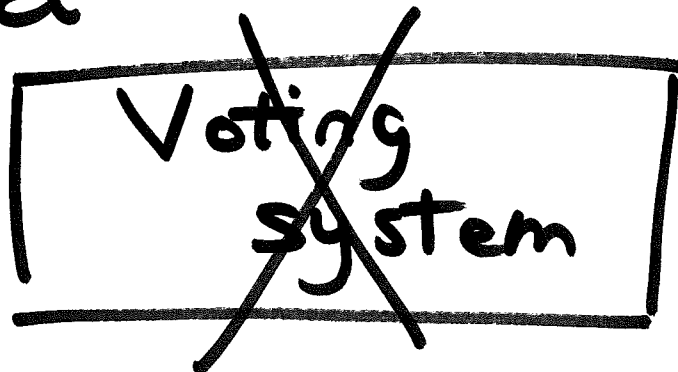
Search



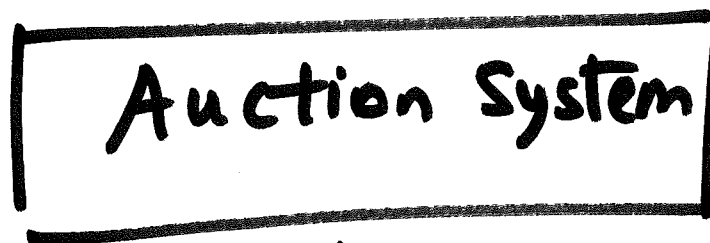
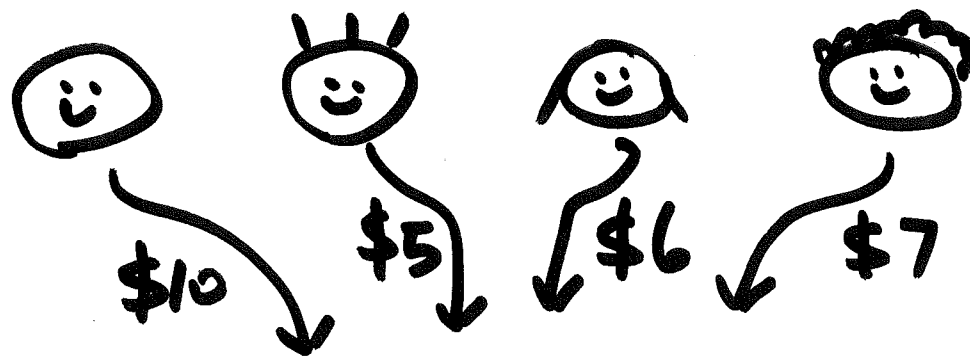
Voting



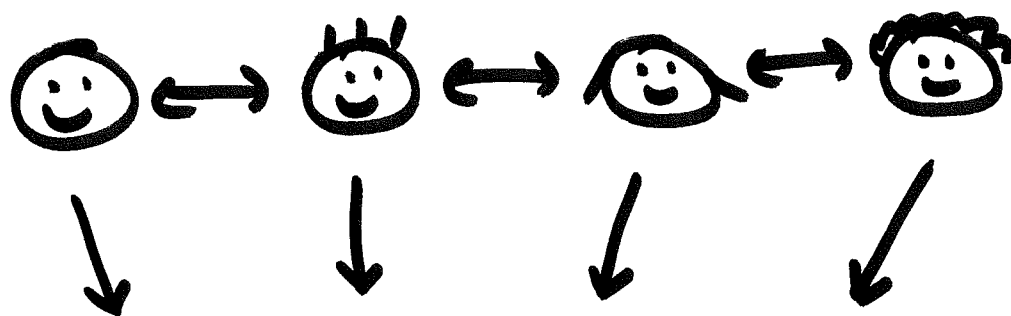
In fact



Private Auction



↓
Winner — A
amt — \$7
(2nd max)



winner = A
amt = \$7

~~Auction System~~