Protection

Growth of Internet → Additional Attacks

Protect from bad guys

Allow access to the good guys

Goal: Privacy

Policy vs <u>Mechanisms</u>

Vs. Real World

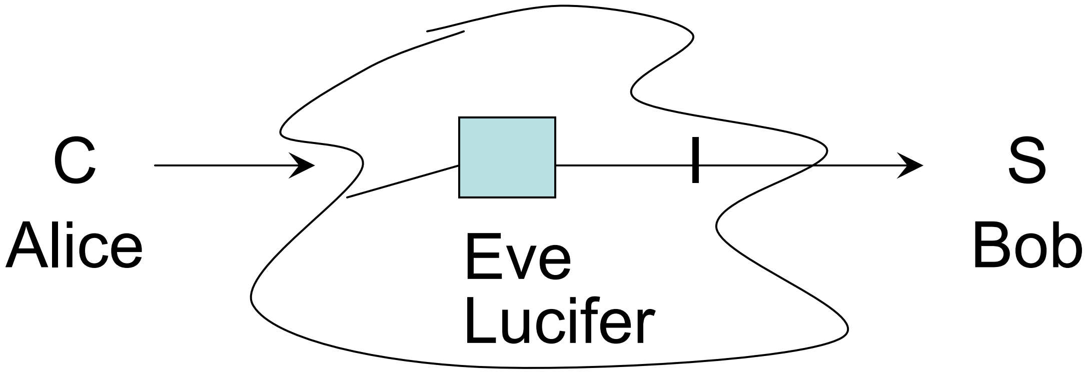
Similar: Locks, encryption
Laws

Differences: dtech/dt
very fast, cheap
Laws

Negative vs. Positive Goals

+ : Sam can access file f (easy)
- : Sam shouldn’t be able to access f

Many security goals are negative



C
Alice

Eve
Lucifer

S
Bob

1) authenticate
2) authorize
3) keep confidential

4) accountability
5) availability

Safety Net Approach

1) be paranoid
   - feedback
   - defend in depth
   - minimize what is trusted ←
2) consider environment
3) plan for iteration
4) keep audit trails

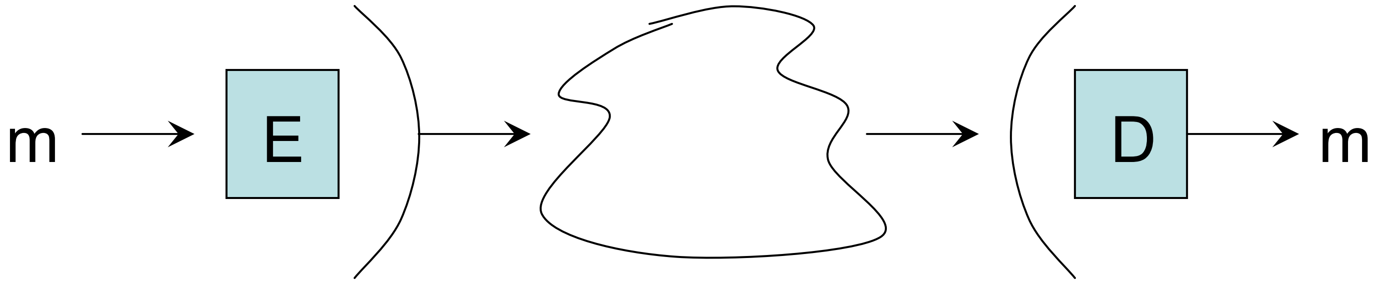
Humans are the weak link

- UI
- good defaults
- least privilege

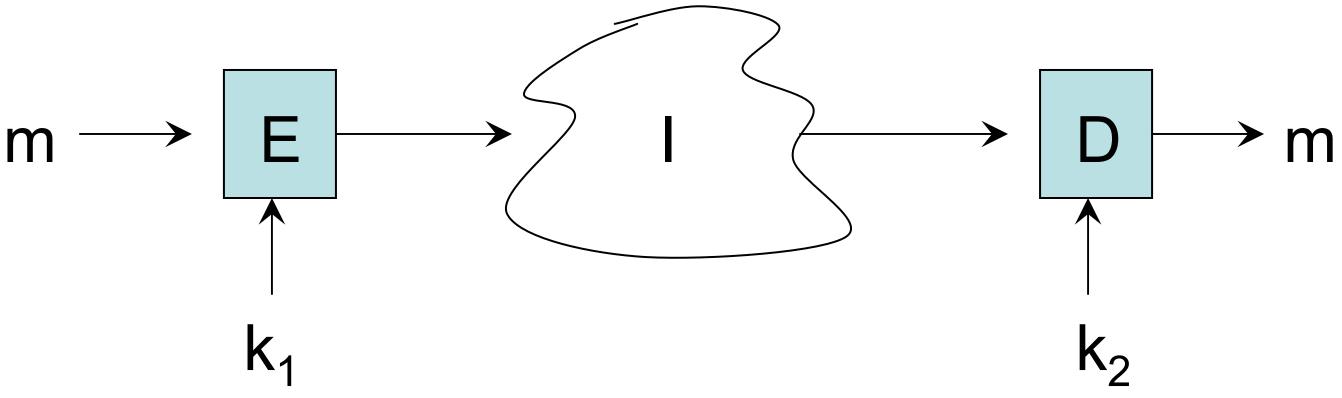
App.

functionality	authenticate	authorize	confid.
primitives	sign verify	ACL	encrypt decrypt
cryptography	cryptographic cypers, hashes		

Closed Design Crypto



Open Design



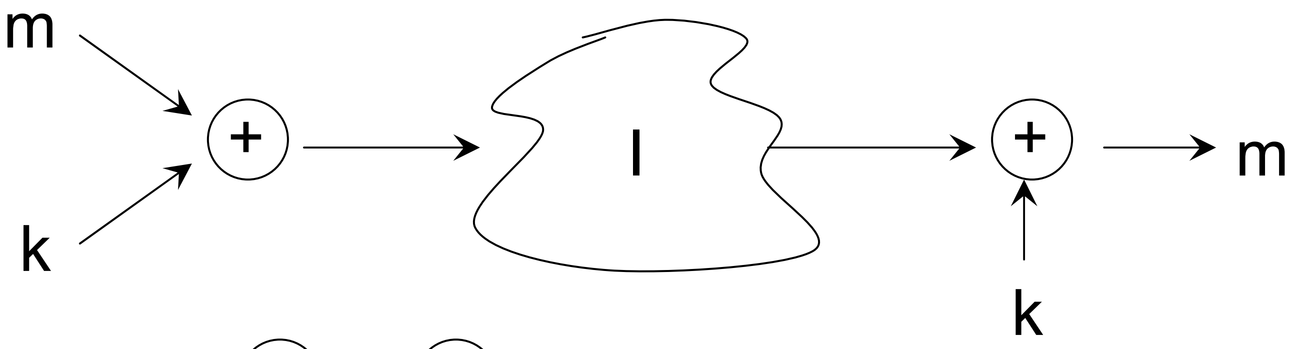
$k_1 = k_2$
shared secret

$k_1 \neq k_2$
public key

One-time Pad

$\oplus$ = xor

xor	0	1
0	0	1
1	1	0



$$(m \oplus k) \oplus k = m$$

RSA Public Key