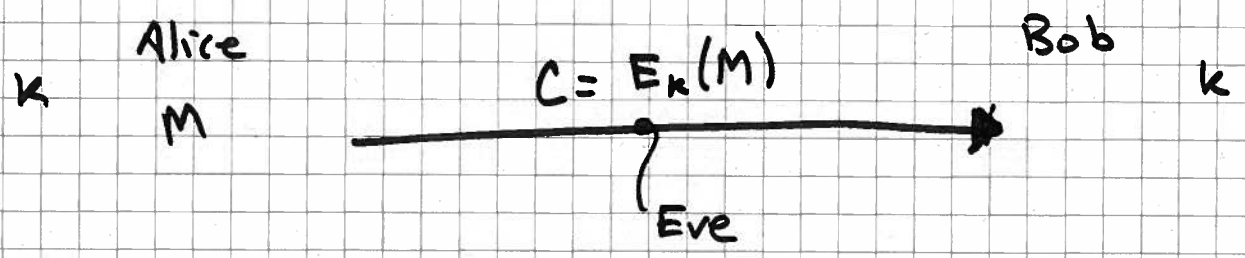
Administrivia – see TA's for "group issues"
- PS #1 due this week
- PS #2 out...

Outline

- ☐ Encryption
- ☐ One-time pad (OTP) & generating random bits
- ☐ RC4 (stream ciphers)
- ☐ Block ciphers
- ☐ DES
- ☐ AES
- ☐ modes of operation

did to here

Encryption (classical) goal: confidentiality



- Bob must know something Eve doesn't
- Eve can't tell $E_k(M_1)$ from $E_k(M_2)$, even if she knows (or chooses) M_1 and M_2 (note: length!) $|M_1| = |M_2|$
- attacks: known ciphertext
  - known PT/CT pairs (same key)
  - chosen PT
  - ...

these assume key is <u>re-used</u>.

But let's do simpler situation first: OTP one-time pad
<u>no key reuse</u> (assumes synchronization...)

One-Time Pad (OTP)

- Vernam 1917 paper-tape based. Patent.
- How it works

Message = 101100 ...
⊕ Pad = 011010 ... (mod-2 addition each column)
Ciphertext = 110110 ...

Pad is random & secret (known only to sender & receiver) & used only once

Note: used by Russian spies (silk handkerchiefs, small pads ...)

Joke: only changes 1/2 the bits - information leaks through!
why not change all the bits? (Desmedt rump session talk)

Proof of security: [Note: insufficient - all c's equally likely, or ... " " " given M ← closer!]

$P(M)$ = probability of message M (may be non-uniform)
= adversaries initial information about M

$P(Pad)$ = probability of pad $= 2^{-n}$ for n-bit pad.

$P(C)$ = probability of observing a given ciphertext

$P(C|M)$ = probability of observing C, given M = message
= probability Pad = $C \oplus M$
$= 2^{-n}$

$$P(C) = \sum_M P(C|M) \cdot P(M)$$

$$= \sum_M 2^{-n} \cdot P(M) = 2^{-n} \cdot \sum_M P(M) = 2^{-n}$$

uniform

P(M|C) = Prob of message, ~~given~~ having seen ciphertext C

= adversary's a posteriori information

$$= \frac{P(C|M) \cdot P(M)}{P(C)} \quad \text{(Bayes' Rule)}$$

$$= \frac{2^{-n} \cdot P(M)}{2^{-n}} = P(M)$$ No change!

⇓

Adversary learns nothing!

⇓

perfect security!

Note: unconditionally secure ≡ no assumptions made or needed about adversary's computing power

≡ information-theoretically secure

(Show brute force doesn't help.)

(Compare to computationally secure ≡ assume adversary has limits to his computing ability.

(e.g. hash fns are only computationally secure).)

Users need to
- generate large secrets
- share them
- keep them secret
- avoid re-using them! (HW) — If $C_1 \oplus C_2 = M_1 \oplus M_2$ if $Pad_1 = Pad_2$

Note: OTP is malleable!

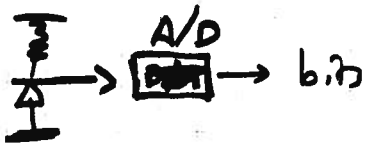
(non-malleability not a requirement)

VENONA, HOMEWORK

How to generate pads?

(my email in/out is ≈ 1 MByte/day)

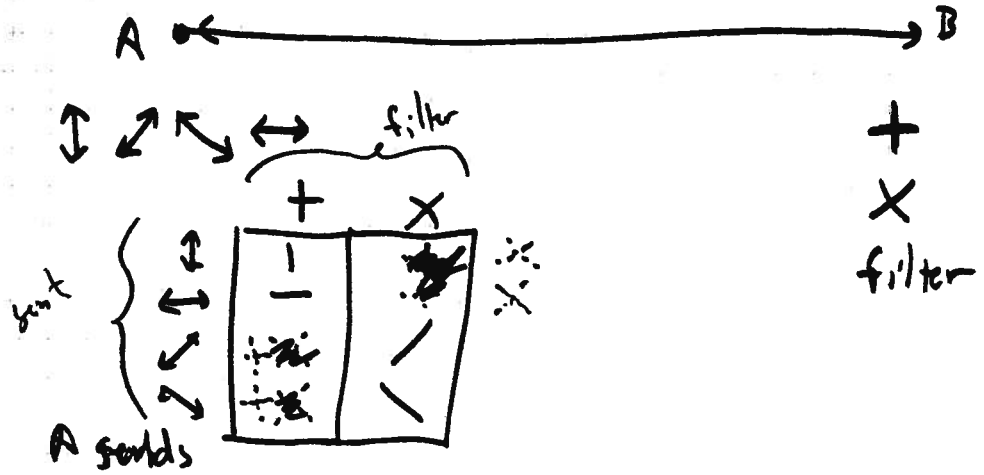
- Coins, dice
- Radioactive sources (old memory chips?)
- Microphone
- Disk speed variations
- Intel chip set — 82802
- Back-biased diodes



- User mouse/typing
- lavarand (lava lamp) laser → LCD
- Alpern & Schneider

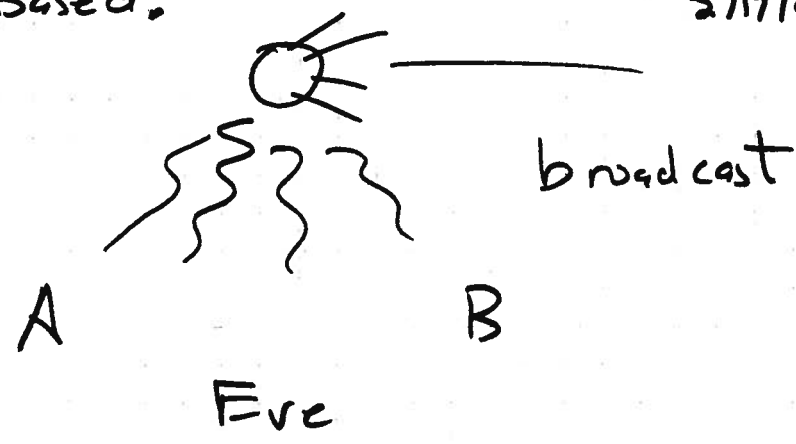
  - eve can't tell who sent message.
  - A & B randomly emit beeps
  - they get shared secret

- Quantum Key Distribution



then they know which bits they have should have in common.

- Satellite Based:



Ideas: channels may be noisy: [A & B with if errors are independent (Maurer)

Eve may have limited memory

- Book-based pad:

take e.g. ~~—~~ 4 or 5 texts (starting points)
XOR together

- "Pseudo-random" pad

"Anyone who considers arithmetical methods of producing random ~~digits~~ digits is, of course, in a state of sin."

(John von Neumann ~~??~~, 1951)

Pseudo-random pad (e.g. RC4)

pseudo-random generator:

256 bits — arbitrarily long...

adversary can't tell PR pads from truly random pads of same length...

RC4: table $S[0..255]$, permutation of 0..255 (init from key)
i, j $0 \le i \le 255$, $0 \le j \le 255$ (pointers into table)

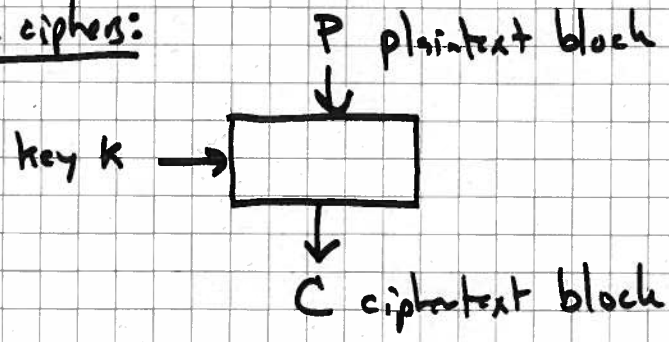
```
i = 0
j = 0
while true do
    i = (i+1) mod 256
    j = (j + S[i]) mod 256
    swap(S[i], S[j])
    output S[(S[i] + S[j]) mod 256]
```

widely used

- setup of S from key is weak; good idea to discard first 1024 bytes of output...

- Note bug implementing $A \leftrightarrow B$ as $A = A \oplus B$, $B = B \oplus A$, $A = A \oplus B$
  doesn't work if A, B the same variable – sets table S to 0's!

Block ciphers:



fixed length of P, C

DES: $|P| = |C| = 64$ bits

AES: $|P| = |C| = 128$ bits

fixed length of K

DES: $|K| = 56$ bits

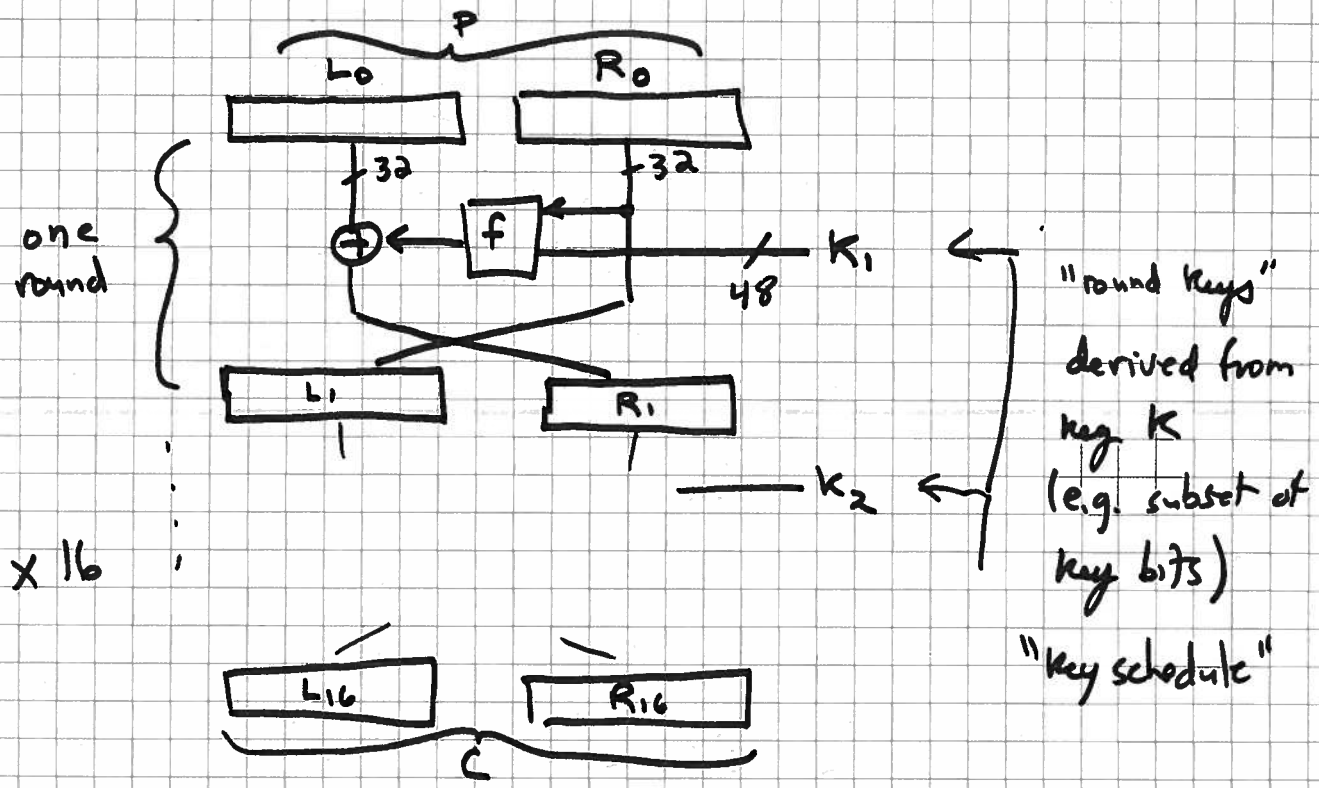
AES: $|K| = 128, 192,$ or 256 bits

Then use "mode of operation" to handle variable-length input.

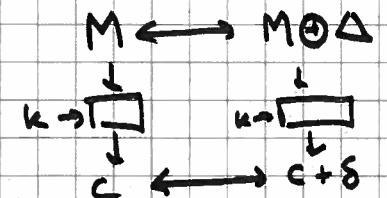
DES

standardized in 70's, now deprecated in favor of AES

Structure "Feistel design", roughly:



- Note: invertible for any f or key schedule
- f uses 8 "S-boxes" mapping 6 bits ⇒ 4 bits for nonlinearity
- key is too short! (breakable now in a few hours...)
- subject to differential attacks:



linear attacks:

$M_3 \oplus M_{15} \oplus C_2 \oplus K_{14} = 0$
with prob $p = 1/2 + \varepsilon$
need $1/\varepsilon^2$ samples to figure out K_{14}...

Matsui 2^{43} PT/CT pairs