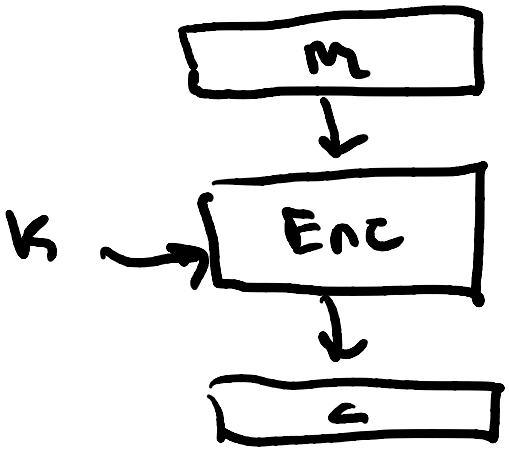
- Block ciphers
- AES
- using AES – CTR
  – CBC

6.857 notes
2021-03-01
L04-2



b = 128 bits

128 bits

Ideal block cipher:

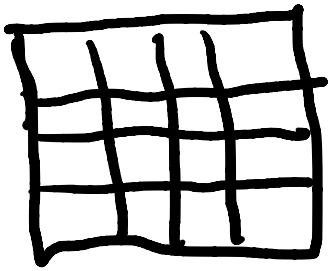
for every K, random permutation of $\{0,1\}^n$ (invertible)

AES

'97 competition

15 competitors RC6, Mars, Twofish, Rijndael

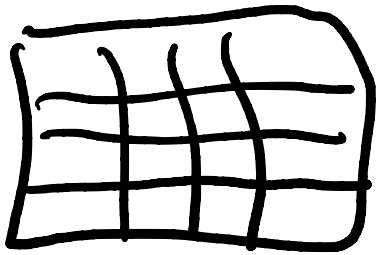
'99 winner Rijndael



4x4 array of 8-bit bytes

k = 128, 192, or 256 bits

rounds = 10, 12, 14 rounds



Derive
11 round keys (128 bits)
from original key K

For each round:

10 rounds:
1. XOR round key into state
2. Substitution byte-wise
3. Rotate rows
4. Mix columns (linear xfrm) $GF(2^8)$

(in last round, do another XOR of key instead)

Output final block

Counter mode

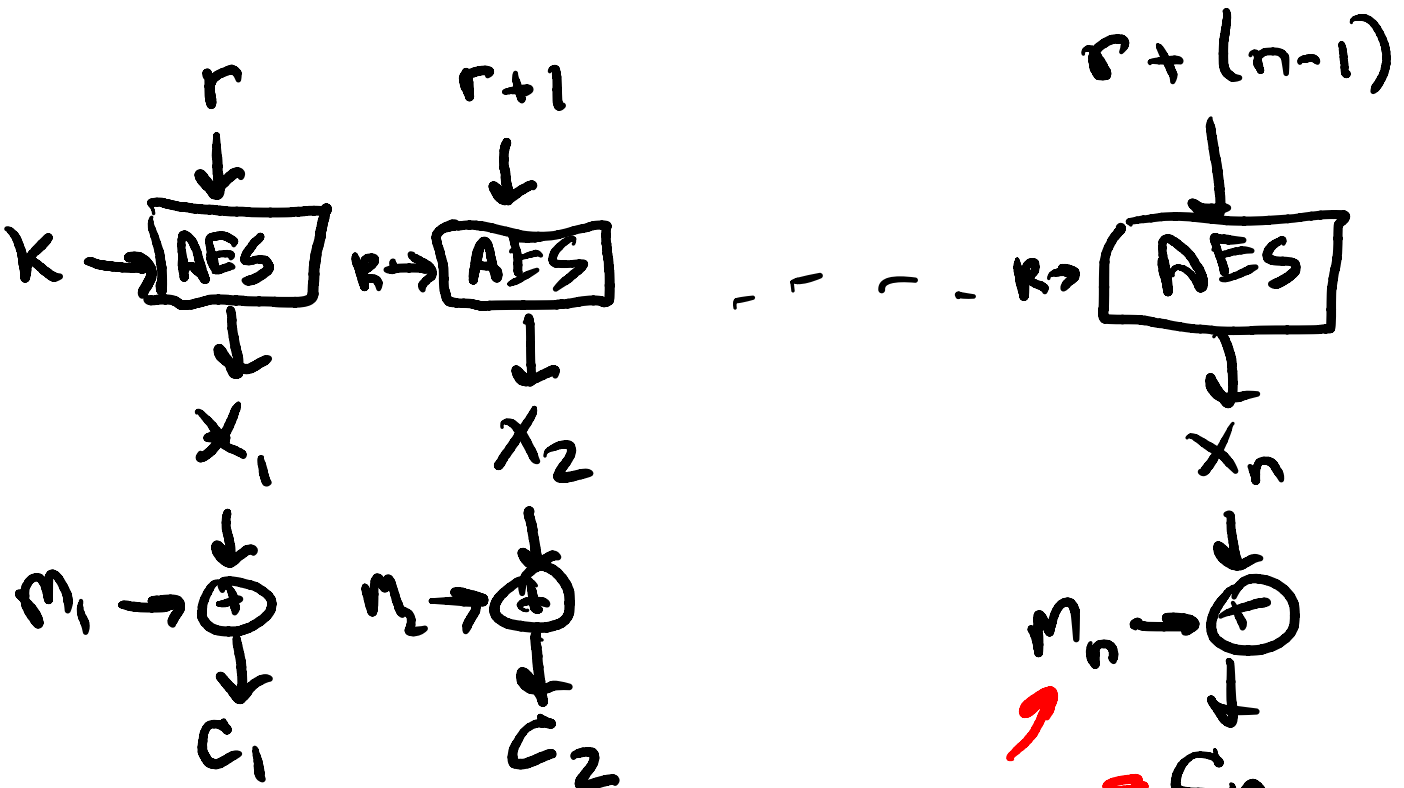
Sender has message $M = M_1, M_2, \ldots, M_n$

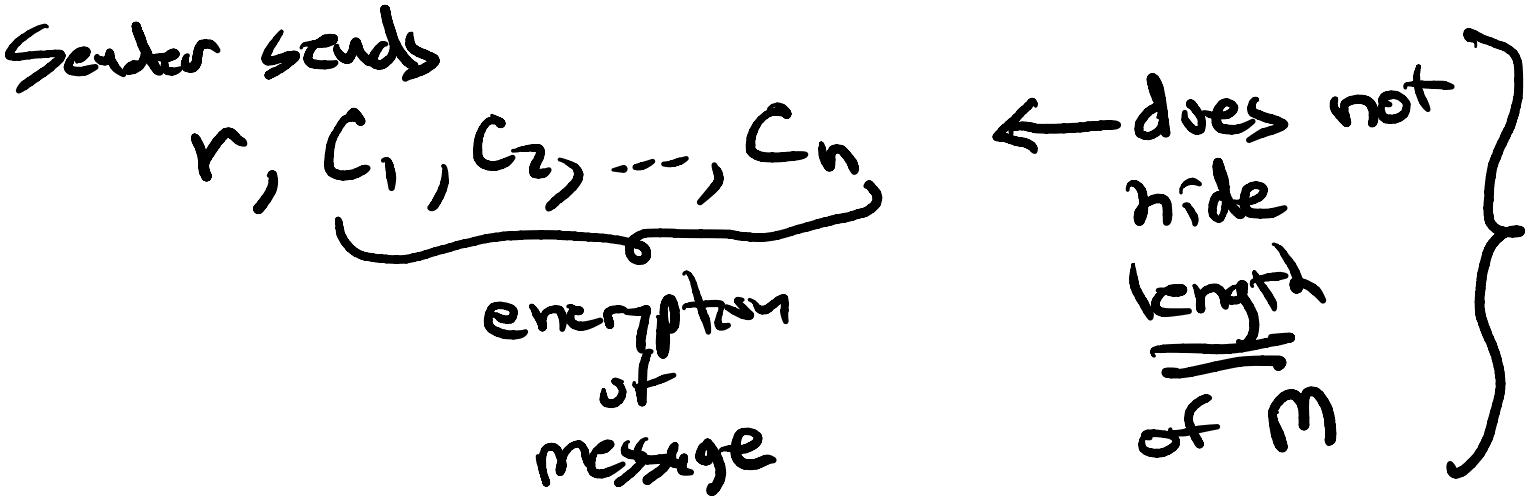
128 bits, 128 bits, $\leq$ 128 bits

M_1: 128 bit blocks

M_n: might be short

Sender generates starting value r for a counter




Sender sends
r, c1, c2, ..., cn
encryption of message
does not hide length of m