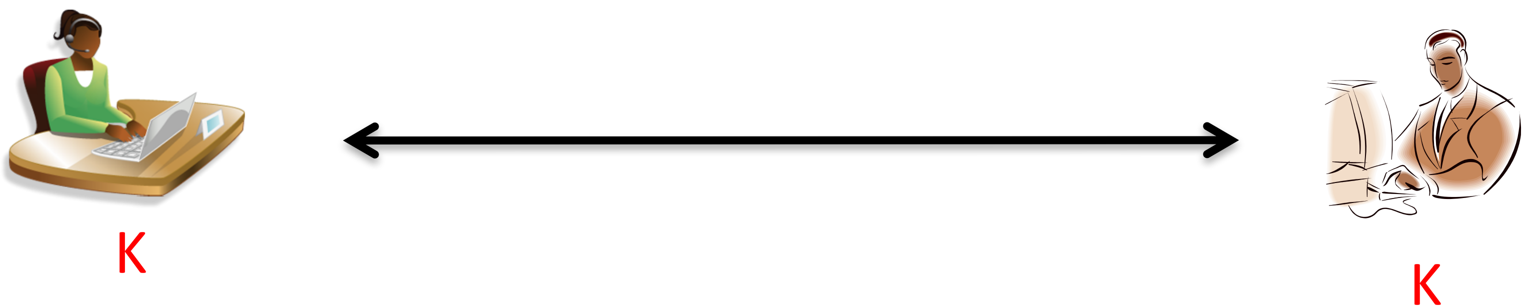
Cryptography (5830)

OTP and Shannon's Perfect Secrecy (KL Chap 2)
Computational security (KL Chap 3)
Basic stream-cipher & block cipher encryption (KL Chap 3)

Symmetric encryption



- Symmetric = secret key shared between sender and recipient
  - Scheme SE = (Kg,Enc,Dec) has three algorithms: Key generation (Kg), Encryption (Enc), Decryption (Dec)
  - Functionality (correctness). Must also be efficient to run all three algorithms
  - Security
    - Capabilities of attacker
    - Attacker goals

One-time pad (OTP)

<u>Kg():</u>
K <-$ $\{0,1\}^L$

Pick a random bit string

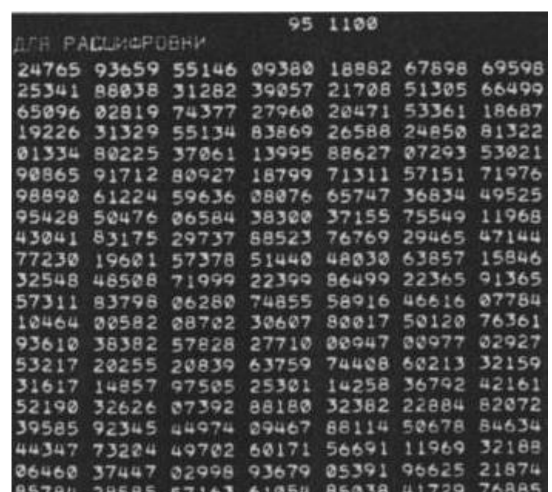
<u>Enc(K,M):</u>
Return M $\oplus$ K

Assume M is L-bit string

<u>Dec(K,C):</u>
Return C $\oplus$ K

Assume C is L-bit string

Part of a CIA OTP used by Soviet diplomat spying for CIA



Shannon's security notion (1949)

Def. A symmetric encryption scheme is perfectly secure if
for all messages M,M' and ciphertexts C

$$\Pr[\,\mathrm{Enc}(K,M) = C\,] = \Pr[\,\mathrm{Enc}(K,M') = C\,]$$

where probabilities are over choice of K

In words:
each message is equally likely to map to a given ciphertext

In other words:
seeing a ciphertext leaks nothing about what message was encrypted

Does a substitution cipher meet this definition? No!

Shannon's security notion (1949)

Def. A symmetric encryption scheme is perfectly secure if for all messages M,M' and ciphertexts C

$$\Pr[\,Enc(K,M) = C\,] = \Pr[\,Enc(K,M') = C\,]$$

where probabilities are over choice of K

Thm. OTP is perfectly secure

For any C and M of length L bits

$$\Pr[\,K \oplus M = C\,] = 1 / 2^L$$

$$\Pr[\,K \oplus M = C\,] = \Pr[\,K \oplus M' = C\,]$$

Shannon's security notion (1949)

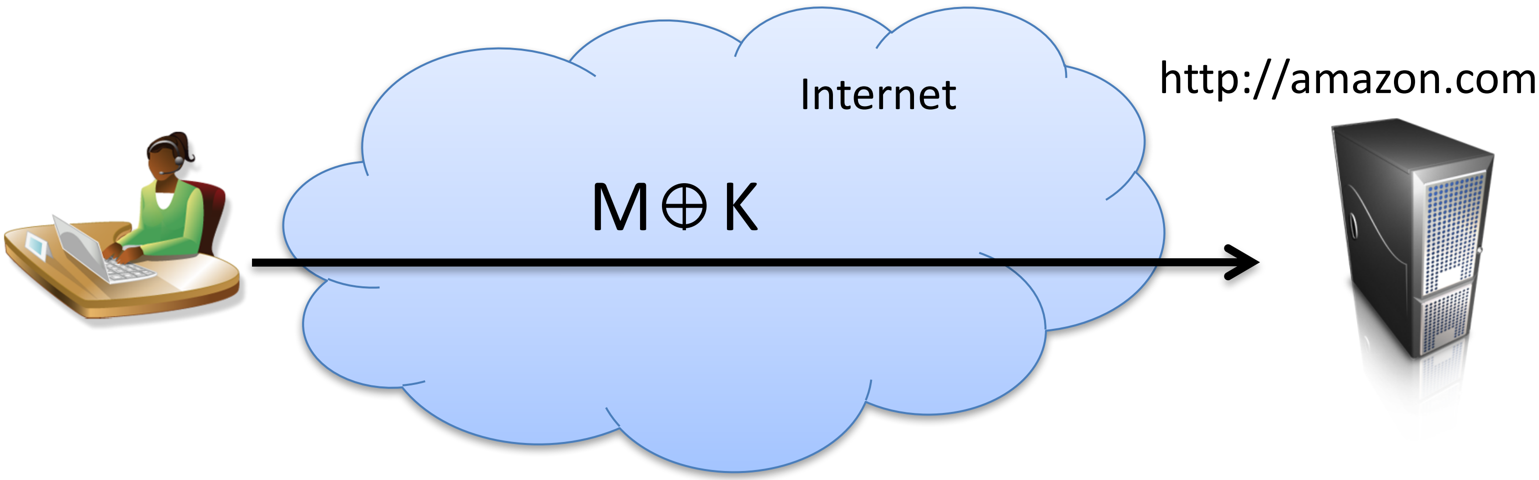
Def. A symmetric encryption scheme is perfectly secure if for all messages M,M' and ciphertexts C

$$\Pr[\ \mathrm{Enc}(K,M) = C\ ] = \Pr[\ \mathrm{Enc}(K,M') = C\ ]$$

where probabilities are over choice of K

Thm. OTP is perfectly secure

Thm. Perfectly secure encryption requires $|K| \geq |M|$



Is OTP good for general-purpose secure channel?

Integrity easily violated

Reuse of K for messages M,M' leaks $M \oplus M'$

Encrypting same message twice under K leaks the message equality

K must be as large as message

Message length revealed

Beyond Shannon

Thm. Perfectly secure encryption requires |K| ≥ |M|

We will ***relax*** the definition of security:

1. Allow tiny adversarial success probability (often written as ϵ)
2. Focus on resource-efficient adversaries (e.g., only those given run time at most t)

Towards computational indistinguishability

Def. A symmetric encryption scheme is perfectly secure if for all messages M,M' and ciphertexts C

$$\Pr[\,\mathrm{Enc}(K,M) = C\,] \;=\; \Pr[\,\mathrm{Enc}(K,M') = C\,]$$

where probabilities are over choice of K

Let's give a game-based formulation of this using an adversary

Let SE = (Kg,Enc,Dec) be a symmetric encryption scheme

Let $\mathcal{A}$ Let be a randomized algorithm, called the adversary

<u>IND(SE,$\mathcal{A}$):</u>

(M_0,M_1) <-\$ $\mathcal{A}$

K <-\$ Kg ; b <-\$ {0,1}

b' <-\$ $\mathcal{A}$ (Enc(K,M_b))

Return (b = b')

IND(SE,$\mathcal{A}$)'s output is 1 if (b = b').

We say then that the adversary succeeded

Def. A scheme SE is perfectly secure if for every $\mathcal{A}$ it is the case that

$$\Pr[\mathrm{IND}(\mathrm{SE},\mathcal{A}) = 1] = 1/2$$

Computational indistinguishability

Def. A symmetric encryption scheme is (t, ϵ)-indistinguishable if for any adversary $\mathcal{A}$ running in time at most t it holds that

$$\Pr[\mathrm{IND}(SE, \mathcal{A}) = 1] < 1/2 + \epsilon$$

1) Tiny adversarial success

2) Computationally limited adversary

Discussion questions:

1) Does (t, ϵ)-indistinguishability model known, chosen message attack? What about chosen ciphertext?
2) Is a OTP (t, ϵ)-indistinguishable?
3) Is a substitution cipher (t, ϵ)-indistinguishable?

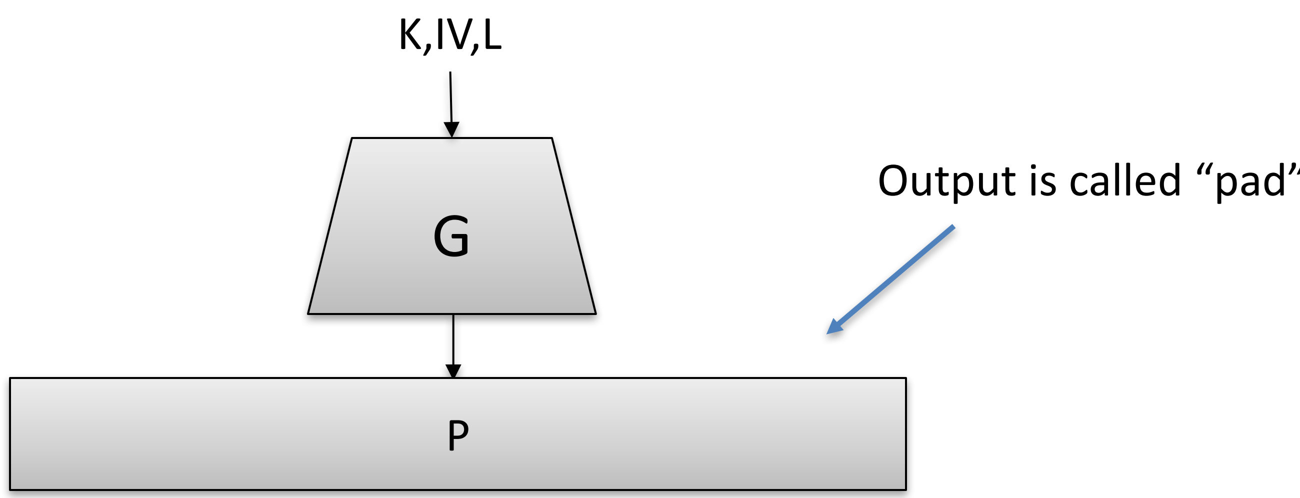
How do we build computationally-secure SE schemes?

- Game plan: need more tools
  - Stream ciphers
  - Block ciphers

Stream ciphers

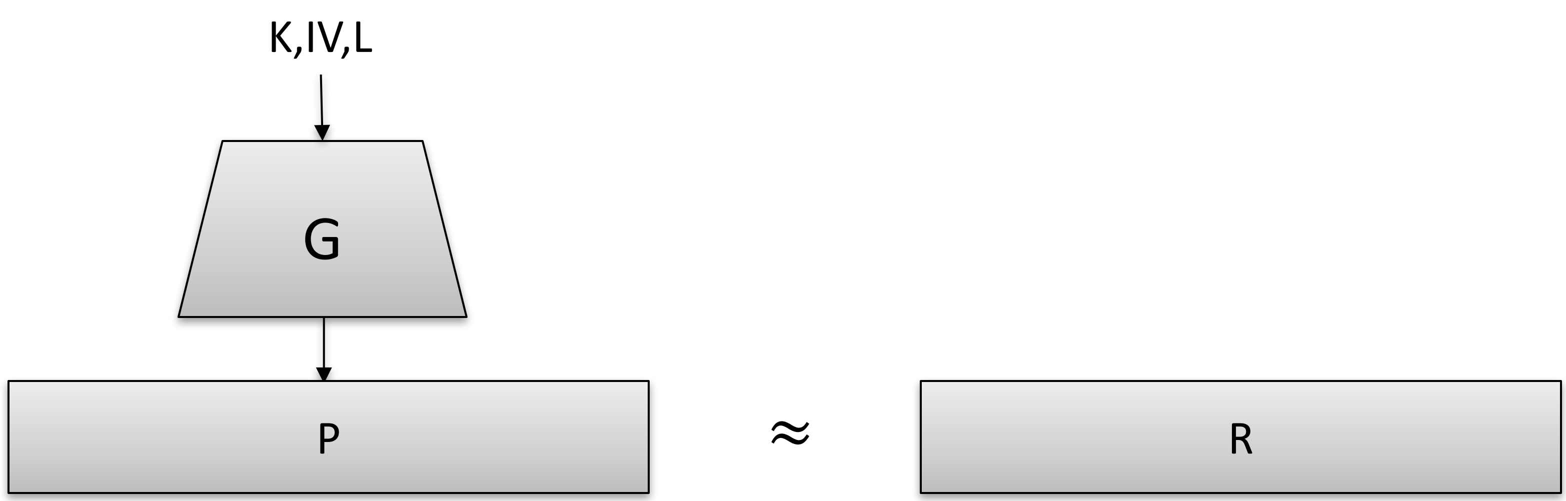
A stream cipher is a pair of algorithms (Kg,G):

- Kg outputs a random key K
- G(K,IV) takes K, additional random value IV (called initialization vector), desired length L, outputs bit string P with |P| = L

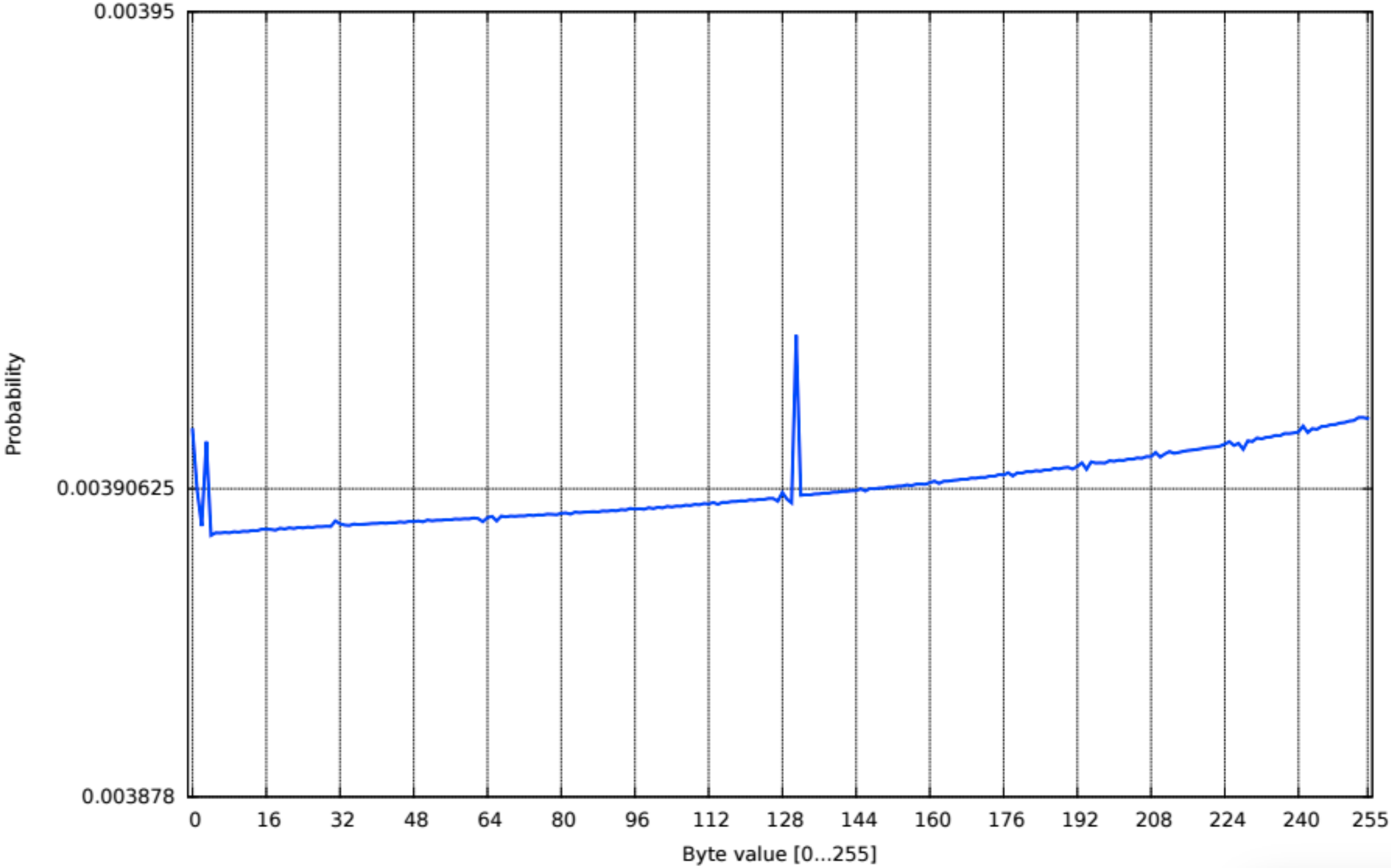


Stream cipher security

Pseudorandom: no attacker limited to time t can distinguish between IV,G(K,IV,L) and random bitstring of length L with probability greater than ϵ



RC4 was up until recently, custom construction of stream cipher.
It is not pseudorandom!


0.00395
0.00390625
0.003878
Probability
0
16
32
48
64
80
96
112
128
144
160
176
192
208
224
240
255
Byte value [0...255]

SE from a stream cipher

Say we have a secure stream cipher. How do we build an SE scheme?

<u>Kg():</u>
K <-\$ $\{0,1\}^k$

Pick a random key

<u>Enc(K,M):</u>
L <- |M|
IV <-\$ $\{0,1\}^n$
Return (IV, G(K,IV,L) $\oplus$ M)

<u>Dec(K,(IV,C)):</u>
L <- |C|
Return G(K,IV,L) $\oplus$ C

Assume ciphertext can be parsed into IV and remaining ciphertext bits

Block ciphers

Family of permutations, one permutation for each key

$$E : \{0,1\}^k \times \{0,1\}^n \text{ --> } \{0,1\}^n$$

Use notation E(K,X) = Y

Define inverse D(K,Y) = X such that D(K,E(K,X)) = X

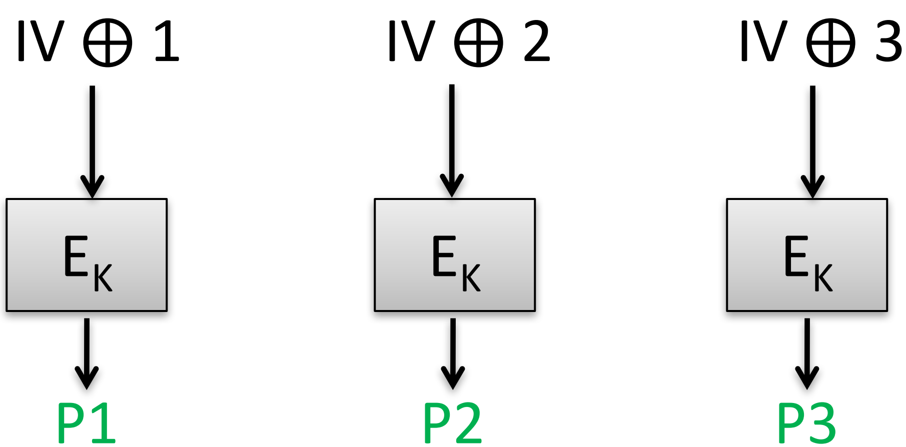
E,D must be efficiently computable

Pick K uniformly at random from $\{0,1\}^k$

CTR mode stream cipher

Counter mode stream cipher CT = (Kg,G) where:

- Kg outputs random k-bit key
- $G(K,IV,L) = E_K(IV \oplus 1) \parallel E_K(IV \oplus 1) \parallel \ \dots \ \parallel trunc(E_K(IV \oplus m))$ where $m = ceil(|M| / n)$



Truncate P3 to get L total bits

SE from a stream cipher

Say we have a secure stream cipher. How do we build an SE scheme?

<u>Kg():</u>
K <-\$ $\{0,1\}^k$

Pick a random key

<u>Enc(K,M):</u>
L <- |M|
IV <-\$ $\{0,1\}^n$
Return (IV, G(K,IV,L) $\oplus$ M)

<u>Dec(K,(IV,C)):</u>
L <- |C|
Return G(K,IV,L) $\oplus$ C

Assume ciphertext can be parsed into IV and remaining ciphertext bits

CTR-mode SE scheme

Say we have a secure stream cipher. How do we build an SE scheme?

<u>Kg():</u>
$K \leftarrow\!\$ \{0,1\}^k$

Pick a random key

<u>Enc(K,M):</u>
$L \leftarrow |M|$; $m \Leftarrow \mathrm{ceil}(L/n)$
$IV \leftarrow\!\$ \{0,1\}^n$
$P \leftarrow E_K(IV \oplus 1) \,\|\, \cdots \,\|\, \mathrm{trunc}(E_K(IV \oplus m))$
Return $(IV, P \oplus M)$

<u>Dec(K,(IV,C)):</u>
$L \leftarrow |C|$; $m \Leftarrow \mathrm{ceil}(L/n)$
$P \leftarrow E_K(IV \oplus 1) \,\|\, \cdots \,\|\, \mathrm{trunc}(E_K(IV \oplus m))$
Return $(IV, P \oplus C)$

Assume ciphertext can be parsed into IV and remaining ciphertext bits

Summary & gameplan

- Perfect secrecy & OTP
- Computational indistinguishability
- Stream ciphers
- Block ciphers

- Next time:
  - Overview of reduction-based proofs

    E secure blockcipher => CTR-mode SE indistinguishable
  - How do we build secure block ciphers?