

One-time pad  
 $keys = \mathcal{M} = \mathcal{C} = \{0, 1\}^l$  (there are  $2^l$  keys)

Thm: The one-time pad has perfect secrecy

Problem: The one-time pad is not practical

Proof:  $E(k, m) = k \oplus m = c$

$D(k, c) = k \oplus c = m$

Goal: Prove that  $\Pr_k [E(k, m_1) = c] = \Pr_k [E(k, m_2) = c]$

for all  $m_1, m_2, c$

Suppose  $E(k, m_1) = c$

then  $k \oplus m_1 = c$

$k = m_1 \oplus c$

so,  $\Pr_k [E(k, m_1) = c] = \frac{1}{2^l}$

this is also true for  $m_2$

Thm: Every encryption scheme

$E: keys \times \mathcal{M} \rightarrow \mathcal{C}$  with perfect secrecy has

$|keys| \geq |\mathcal{M}|$

Proof: Fix  $c \in \mathcal{C}$  s.t.  $c \in \text{Range}(E)$

Let  $D = \{D(k, c) : k \in keys\}$

then,  $|D| \leq |keys|$

Also,  $\exists k, m$  s.t.  $E(k, m) = c$

so,  $\Pr_k [E(k, m) = c] \neq 0$

By perfect secrecy,

$\Pr_k [E(k, m) = c] \neq 0$

$\forall m' \in \mathcal{M}$

Hence,  $D = M$

So,  $|M| = |D| \leq |keys|$

Conclusion: Perfect secrecy is impractical

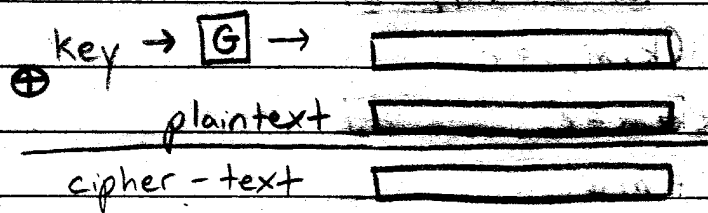
### Stream Ciphers

keys =  $\{0, 1\}^L$

G is a deterministic

$M = C = \{0, 1\}^L$

number generator



G:

- is deterministic

- must have bigger output than input

### Example

unsigned int state;

int rand(void)

{

state = 322349 \* state + 45656749;

return state % 2;

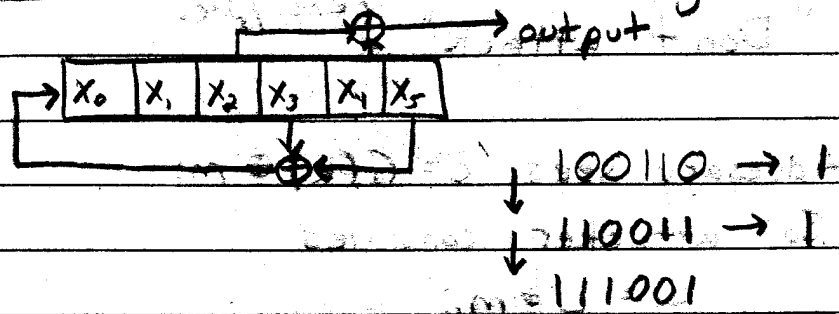
}

even  $\rightarrow$  odd  $\rightarrow$  even  $\rightarrow$  odd  $\rightarrow$  ...

So, the output of  $\text{rand}()$  is one of

$\begin{cases} 01010101\dots \\ 10101010\dots \end{cases}$

Example: Linear Feedback Shift Register (LFSR)



Attack on LFSR

$$\text{output } b_0 = x_2 \oplus x_4$$

$$b_1 = x_1 \oplus x_3$$

$$b_2 = (x_5 \oplus x_2) \oplus x_4$$

$$b_3 = (x_4 \oplus x_5) \oplus x_2$$

$$b_4 = (x_3 \oplus x_4) \oplus x_0$$

$$b_5 = (x_2 \oplus x_3) \oplus (x_3 \oplus x_5)$$

can recover key by solving linear equations

solution:  $O(n^3)$

What do we want from a good PRG?

- look random

- be uniform

- can't compute key from outputs

- can't predict future outputs from output

- can't compute past outputs from output

Consider scenario where the sender sends either

"Let's attack" }  
"Don't attack" } encrypted

Adversary sees  $c = G(k) \oplus m_i$

So, attacker computes

$$S_1 = c \oplus m_1$$

$$S_2 = c \oplus m_2$$

Suppose  $G$  always outputs a prime number

$$\text{Suppose } S_1 = 17 * 3042$$

$\Rightarrow$  Sender sent  $m_1$ !

Goal: output of  $G$  is indistinguishable from randomly chosen bit string

### Distinguishability

A distribution  $D$  on set  $S$  is a function

$$D: S \rightarrow [0, 1]$$

where  $D(x)$  is the probability of choosing  $x$

We say  $X \leftarrow D$  to mean  $x$  is chosen

according to  $D$

Ex. The uniform distribution  $U$   
on  $\{1, \dots, 10\}$

$$Pr[X \leftarrow U; X=4] = \frac{1}{10} \quad \therefore$$

Ex. Let  $B$  = distribution of the # of heads  
after flipping 2 coins

$$Pr[X \leftarrow B; X=0] = \frac{1}{4}$$

$$Pr[X \leftarrow B; X=1] = \frac{1}{2}$$