

# One-Time Pad

OTP:  $\text{Enc}(k, m) = k \oplus m$   
 $\text{Dec}(k, c) = k \oplus c$

## Reminder:

pre-class Canvas discussions  
worth 10% of grade  
(graded -for good-faith effort)

Correctness:  $\text{Dec}(k, \text{Enc}(k, m)) = m$

Security: for all  $m$ : output of

```
VIEW( $m$ )
 $k \leftarrow \{0,1\}^{\lambda}$ 
return  $k \oplus m$ 
```

$$m \in \{0,1\}^{\lambda}$$

set of all bit strings of length  $\lambda$

is uniformly distributed

## Enc

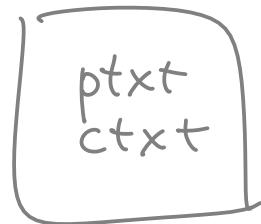
sender's perspective  
know  $k$   
know  $m$

## VIEW

eavesdropper's perspective  
random / secret  $k$   
see only  $c$

Security of OTP only applicable when:

key chosen uniformly  
key used to encrypt just one ptxt  
and used nowhere else  
eavesdropper sees ctxt



## Questions:

Reusing OTP key: use same  $k$  to encrypt  $> 1$  ptxt  
what goes wrong? [Ex 1.5]

$$\begin{aligned} C_1 &= k \oplus m_1 \\ C_2 &= k \oplus m_2 \end{aligned}$$

same

Ex:

$$\begin{array}{l} c_1 = 001101 \\ c_2 = 011000 \end{array} \quad \left. \begin{array}{c} \\ \\ \uparrow \uparrow \uparrow \end{array} \right\} \oplus 010101 \quad \begin{array}{c} \uparrow \uparrow \uparrow \end{array}$$

$m_1$  &  $m_2$  agree in these positions

Tip: 2 expressions w/ XOR, common term  
XOR both together, common term cancels

$$\begin{aligned} c_1 \oplus c_2 &= (\cancel{k} \oplus m_1) \oplus (\cancel{k} \oplus m_2) \\ &= \underbrace{m_1 \oplus m_2}_{\text{info about pts only}} \end{aligned}$$

eavesdropper can do this

If  $m_1 \oplus m_2$  has 1 in some position  
 $\Leftrightarrow m_1$  &  $m_2$  have different bits  
in that position

## Brute force on OTP [ex 1.4]

Idea: given  $c$ .

try all possible  $k$

for each  $k$ , compute  $m = \text{Dec}(k, c)$

when you find correct  $k$ , stop

(and you've learned  $m$ !)

how?

Ex: I encrypted  $m_1$  under OTP, and  $m_2$  w/  
same key  
result is 011

Brute force:

$$k = 000 \Rightarrow m_1 = 011 \quad m_2 = 111$$

$$k = 001 \Rightarrow m_1 = 010 \quad m_2 = 110$$

$$010 \quad 001 \quad 101$$

$$011 \quad 000 \quad 100$$

$$100 \quad 111 \quad \vdots$$

$$101 \quad 110 \quad \vdots$$

$$110 \quad 101 \quad \vdots$$

$$111 \quad 100 \quad \vdots$$

haven't narrowed down  
anything

Before you saw ctxt, any  $m \in \{0,1\}^3$  is  
equally valid

After you saw ctxt, same!

c known, { if you learn correct k, can solve for m  
if you learn correct m, can solve for k

but neither k nor m are known

Is longer OTP more secure than short OTP?

OTP w/ 5 bits  $\Rightarrow$  can guess key w/ prob  $\frac{1}{2^5}$

OTP w/ 100 bits  $\Rightarrow$  ...

$\frac{1}{2^{100}}$

even w/o OTP, if you know I'm sending  
... 5 bits, you can guess w/ prob  $\frac{1}{2^5}$

.. 100

$\frac{1}{2^{100}}$

OTP security doesn't say that anything is hard to guess  
only that distribution is uniform

Ex: Enc of  $m = 01111001$  is  $c = 11011000$

[Ex 1.1] what is Enc of  $m' = 10000110$  under  
same key?

$$\begin{aligned} m \oplus m' \oplus c &= m \oplus m' \oplus (m \oplus k) \\ &= m' \oplus k \end{aligned}$$