One-Time Pad

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

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

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

Security: for all m: output of

```
VIEW(m)
  k ← {0,1}^λ
  return k ⊕ m
```

is uniformly distributed

$m \in \underbrace{\{0,1\}^\lambda}_{\text{set of all bit strings of length } \lambda}$

Enc	VIEW
sender's perspective	Eavesdropper's perspective
know k	random / secret k
know m	see only c

ptxt
ctxt

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]

same

$$c_1 = k \oplus m_1$$
$$c_2 = k \oplus m_2$$

Ex:

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

m_1 & m_2 agree in these positions

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

$$c_1 \oplus c_2 = (\cancel{k} \oplus m_1) \oplus (\cancel{k} \oplus m_2)$$

$$= \underbrace{m_1 \oplus m_2}_{\text{info about ptxts only}}$$

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 $m = Dec(k, c)$
when you find correct k, stop and you've learned m!

how?

Ex: I encrypted m_1 under OTP, result is 011

and m_2 w/ same key 111

$m_1 \oplus m_2 = 100$

Brute force:

$k = 000 \Rightarrow$	$m_1 = 011$	$m_2 = 111$
$k = 001 \Rightarrow$	$m_1 = 010$	110
010	001	101
011	000	100
100	111	⋮
101	110	
110	101	
111	100	

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 $\Rightarrow$ . . . $1/2^{100}$

even w/o OTP, if you know I'm sending

... 5 bits, you can guess w/ prob $1/2^5$

.. 100 $\qquad$ $1/2^{100}$

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

Ex: Enc of $\overset{m}{01111001}$ is $\overset{c}{11011000}$

[Ex 1.1] what is Enc of $\underset{m'}{10000110}$ under same key?

$$m \oplus m' \oplus c = \cancel{m} \oplus m' \oplus (\cancel{m} \oplus k)$$

$$= m' \oplus k$$