Intro to modern crypto + perfect security

Recommended reading:

Katz-Lindell, Chapter 1, Sections 2.1 - 2.3

Barak, Section 0.2

Modern Cryptography:

→ Techniques for securing information and computation

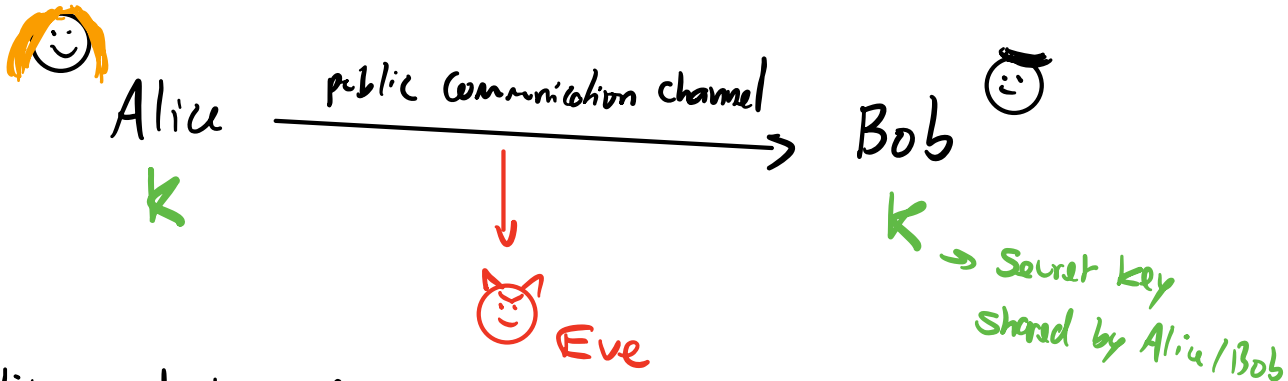
→ Rigorous definitions of security

→ Rigorous proofs of security

* Beautiful mathematics!
  Crown jewel of the theory of computation
  Connections to algebra, combinatorics, geometry, number theory, complexity theory, information theory

* Amazing practical impact!
  Everyone uses crypto on a daily basis, even if they don't realize it.
  Widely deployed cryptographic algorithms are developed based on the rigorous theory we discuss in this course.

The starting point: Secret-key Encryption



Alice wants to send a message m to Bob over the public channel. Eve should not learn anything about the message.

Before we think about how to do this, we need to first think about how to formalize the intuition above!

Def (encryption scheme).

An encryption scheme is specified by a tuple of algorithms (Enc, Dec, Gen), a message space $\mathcal{M}$, a keyspace $\mathcal{K}$, and a ciphertext space $\mathcal{C}$ such that:

- Gen is a probabilistic algorithm that outputs a key k from $\mathcal{K}$, independently of the message to be encrypted.
- Enc receives as input the key k and a message m and outputs a ciphertext $c = Enc(k, m) \in \mathcal{C}$
- Dec receives as input the key k and a ciphertext c and outputs the decryption $Dec(k, c) \in \mathcal{M}$.

Correctness: We require that

$$\Pr(\mathrm{Dec}(k, \mathrm{Enc}(k,m)) = m) = 1$$

for all messages $m \in \mathcal{M}$, keys $k \in \mathcal{K}$.

Perfect security (Shannon, 1949):

Intuition: Ciphertext should not reveal <u>any</u> statistical info about message to someone who doesn't know the key.

Not sufficient to just say "adversary can't guess the full message given $c = \mathrm{Enc}(k,m)$."

An encryption scheme is perfectly secure if for every random variable M supported on $\mathcal{M}$ and for K the random variable denoting the output of Gen we have that M and $C = \mathrm{Enc}(K, M)$ are independent random variables.

This means that

$$\Pr(M = m \mid C = c) = \Pr(M = m)$$

for all c in the support of C (ie, all c's s.t. $\Pr(C=c) > 0$).

So knowing C reveals no info about M.

Now that we have a good definition of Security, can we construct an encryption scheme that satisfies it?

One-Time Pad (Vernam 1917):

Fix $n \in \mathbb{N}$. Set $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$

Gen: Sample k uniformly at random from $\{0,1\}^n$

$Enc(k, m) = k \oplus m = (k_1 \oplus m_1, \dots, k_n \oplus m_n)$

with $a \oplus b = a + b \bmod 2 = \begin{cases} 1, \text{ if } a \neq b \\ 0, \text{ if } a = b \end{cases}$

$Dec(k, c) = k \oplus c$

Correctness of OTP:

$$Dec(k, Enc(k, m)) = k \oplus Enc(k, m) = k \oplus (k \oplus m) = m$$

Perfect security of OTP:

We need to show that for any random variable M, $m \in \mathcal{M}$, $c \in \mathcal{C}$, we have $Pr(M = m, Enc(K, M) = c) = Pr[M = m] \cdot Pr(Enc(K, M) = c)$

$$\begin{aligned}
Pr(M=m, Enc(K,M)=c) &= Pr(M=m, Enc(K,m)=c) \\
&= Pr(M=m) \cdot Pr(Enc(K,m)=c) \\
&= Pr(M=m) \cdot Pr(K \oplus m = c) \\
&= Pr(M=m) \cdot Pr(K = c \oplus m) \\
&= \underline{2^{-n} \cdot Pr(M=m)}
\end{aligned}$$

$$\begin{aligned}
Pr(M=m) \cdot Pr(Enc(K,M)=c) &= Pr(M=m) \cdot \sum_m \underbrace{Pr(M=m, Enc(K,M)=c)}_{2^{-n} \cdot Pr(M=m)} \\
&= Pr(M=m) \underbrace{\sum_m 2^{-n} Pr(M=m)}_{2^{-n}} \\
&= \underline{2^{-n} \cdot Pr(M=m)}
\end{aligned}$$

▨

What's good about the OTP?

Eve really learns nothing about m!

What's bad about the OTP?

Key can only be used once...

Key is as long as the message...

Can we come up with better perfectly secure encryption schemes?

Not really!

Theorem: Every perfectly secure encryption scheme must have $|K| \geq |M|$.

Proof: Let M be uniformly distributed over $\mathcal{M}$.
Without loss of generality, can assume that $Pr(C=c)>0$ for all $c \in \mathcal{C}$ $\rightsquigarrow$ $\mathcal{C} = Enc(K, M)$.

Observation 1: For every $m \in \mathcal{M}$, $c \in \mathcal{C}$ there is $k \in K$ s.t. $Dec(k,c) = m$. Otherwise perfect security is not satisfied.

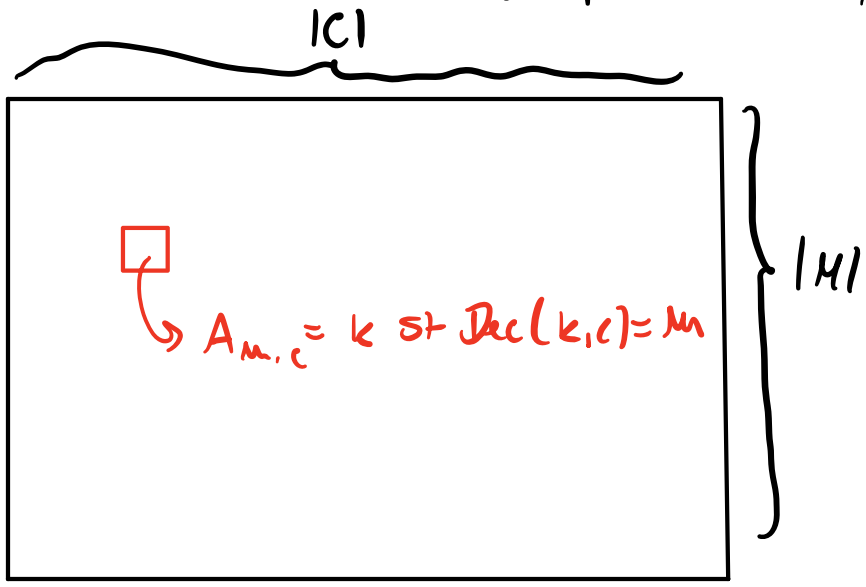
Indeed, if there is no k s.t. $Dec(k,c) = m$ then

$$Pr(M=m, C=c) = 0 \neq Pr(M=m)\,Pr(C=c)$$

Observation 2: By correctness, we must have

$$Dec(k,c) \neq Dec(k',c) \text{ for all } k \neq k',\ c \in C.$$

$A =$



Fix any $c \in C$. This corresponds to a column of A.

By Obs 1 there is a key in every entry of this column

By Obs 2 every entry in this column has a distinct key

Since a column has $|M|$ entries, this can only happen if $|K| \geq |M|$. ▨

So... is this the end of the course?

How can we build crypto with shorter keys?!?!