"Modern cryptography is one great example of the incredible economic consequences of curiosity-driven, theoretical research."

—Avi Wigderson, Math + Computation

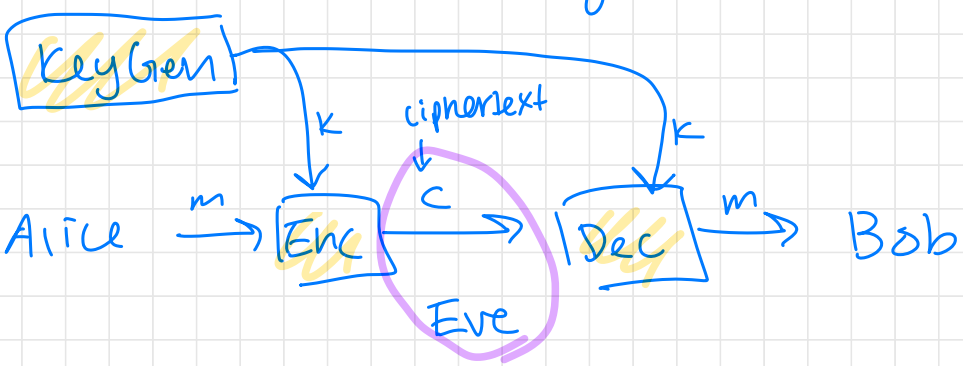
P: problems solvable in polynomial time

Encryption

plaintext ↓

Alice has message m to send to Bob over unsecure channel

Let Enc and Dec be algorithms that take in and return strings



KeyGen: generates random key k

Kerchoffs' Principle: System must be secure, even if Eve has knowledge of all algorithms.

→ Security of system should be concentrated in key, not algorithms.

KeyGen:

return random $k \in \{0,1\}^\lambda$

Enc$(k, m \in \{0,1\}^\lambda)$:

return $k \oplus m$

$\oplus$ = XOR = exclusive or

$$\begin{array}{r} 101 \\ \oplus\ 111 \\ \hline 010 \end{array}$$

1 if diff
0 if same

Dec$(k, c \in \{0,1\}^\lambda)$

return $k \oplus c$

	11101111101111100011	(m)
$\oplus$	00011001110000111101	(k)
	11110110011111011110	$(c = \text{Enc}(k, m))$

	00001001011110010000	(c)
$\oplus$	10010011101011100010	(k)
	10011010110101110010	$(m = \text{Dec}(k, c))$

Property 1: Correctness

For all $k, m \in \{0,1\}^\lambda$, Dec$(k,$ Enc$(k,m)) = m$.

Pf $\text{Dec}(k, \text{Enc}(k,m)) = \text{Dec}(k, k \oplus m)$ def of Enc

$= k \oplus (k \oplus m)$ def of Dec

$= (k \oplus k) \oplus m$ assoc. of $\oplus$

$= 0^\lambda \oplus m$ $\quad X \oplus X = 0$

$= m$ $\quad 0 \oplus x = x$

Property 2: Security

Whatever is knowable about m given C is also knowable without C.

Eavesdrop($m \in \{0,1\}^\lambda$):

$k =$ random $\in \{0,1\}^\lambda$
return $c = k \oplus m$

EAVESDROP(010):		
Pr	*k*	*output* $c = k \oplus 010$
1/8	000	010
1/8	001	011
1/8	010	000
1/8	011	001
1/8	100	110
1/8	101	111
1/8	110	100
1/8	111	101

EAVESDROP(111):		
Pr	*k*	*output* $c = k \oplus 111$
1/8	000	111
1/8	001	110
1/8	010	101
1/8	011	100
1/8	100	011
1/8	101	010
1/8	110	001
1/8	111	000

uniform dist. on m

Eavesdrop2($m_1, m_2 \in \{0,1\}^\lambda$)

$k =$ random $\in \{0,1\}^\lambda$
return $c_1 = k \oplus m_1$, $c_2 = k \oplus m_2$

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

$= (m_1 \oplus k) \oplus (k \oplus m_2)$ comm. of $\oplus$

$= m_1 \oplus (k \oplus k) \oplus m_2$ assoc. of $\oplus$

$= m_1 \oplus 0^\lambda \oplus m_2$

$= m_1 \oplus m_2$

If $\lambda = 2$, $c_1 \oplus c_2 = 11$

$$\begin{array}{ccccc} 11 & 00 & 01 & 10 & 11 \\ 00 & 11 & 10 & 01 & 11 \\ \hline & & & & 00 \end{array}$$

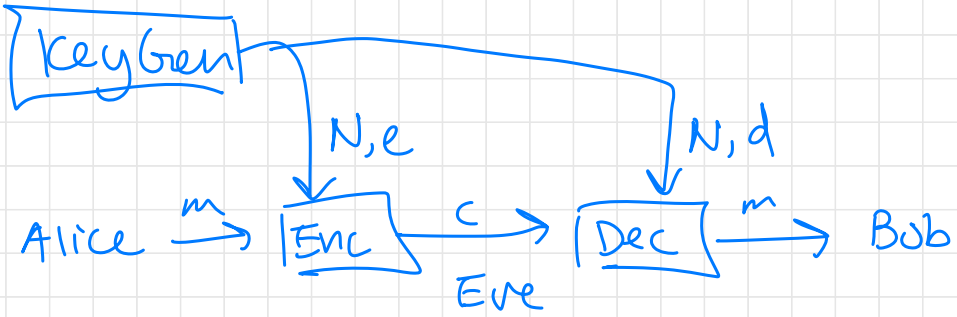
One-time Pad

- one-time use of k
- $len(k) = len(m) = \lambda$
- if we could send k securely, why not send m securely?

(Computational) Property 2

Whatever is efficiently computable about m given c is also efficiently computable without c.

RSA Encryption


KeyGen
N, e
N, d
Alice
m
Enc
c
Dec
m
Bob
Eve