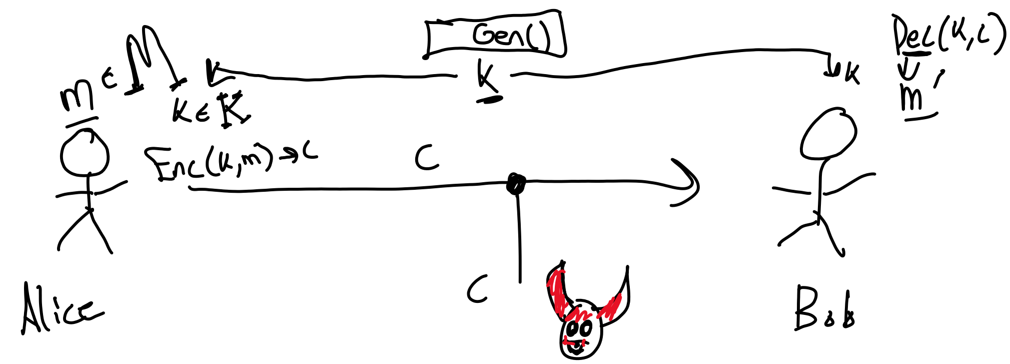
One time pads, symmetric encryption

Monday, August 23, 2021 12:18 PM

Model of Symmetric Encryption:



Defn: A Symmetric key encryption is:

a tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, Gen, Enc, Dec)$

message space, ciphertext space, keyspace

$Gen(; z) \to$ random bitstream used by Gen

system

- $Gen() \to \mathcal{K}$
- $Enc : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
- $Dec(k \in \mathcal{K}, c \in \mathcal{C}) \to m \in \mathcal{M}$

Satisfying:

Properties

- Correctness "decode is inverse of encode" "same key can be used to encrypt and decrypt" "decrypt with the same key as encrypt gives the same message"

$$\forall m \in \mathcal{M}.\ \Pr\left[\begin{array}{l} k \leftarrow Gen() \\ c \leftarrow Enc(k,m) \\ m' \leftarrow Dec(k,c) \\ \hline \text{return } m' = m \end{array}\right] = 1$$

alt: $\forall m, k$

- Secrecy definition "having c w/o k means cannot recover m"

m = "my bank password is xabx and my dog's name is ////"

One Time Pad: $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^{\ell}$ uniform sample $k \leftarrow \mathcal{D}$

- Gen(): $k \xleftarrow{\$} \mathcal{K}$

bitwise Xor

- Enc(k,m): return $c = m \oplus k$

- Dec(k,c): return $m' = c \oplus k$

This satisfies
- correctness
- secrecy...

Proof: $(m \oplus k) \oplus k = m$

Ex Half Time Pad $\mathcal{C} = \mathcal{M} = \{0,1\}^{2\lambda}$ $\mathcal{K} = \{0,1\}^{\lambda}$

(Broken)

- Gen: $k \xleftarrow{\$} \mathcal{K}$

Concat.

- $\text{Enc}(k,m) = m \oplus k \cdot k$
- $\text{Dec}(k,c) = c \oplus k \cdot k$

$\lambda = 1$

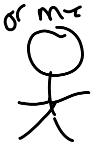
Counterexample: if $c = 11$

we learn $m \in \{00, 11\}$

$m_1 \; m_2$

$k \; k$

$m = 00$
or $m = 01$



$m_1 \oplus k = 1$

$m_2 \oplus k = 1$

$m_1 \oplus m_2 \oplus k \oplus k = 1 \oplus 1 = 0$

$m_1 \oplus m_2 = 0$

- Uniform Ciphertexts property of One Time Pad

$$\forall m. \left\{ \begin{array}{l} k \leftarrow \text{Gen}() \\ c \leftarrow \text{Enc}(k,m) \\ \text{return } c \end{array} \right\} = \text{Uniform}(\mathcal{C})$$

- $\boxed{\text{Perfect Secrecy.}}$

$$\Rightarrow \forall m_1, m_2, \left\{ \begin{array}{l} k \leftarrow \text{Gen}() \\ \text{Enc}(k, m_1) \end{array} \right\} = \left\{ \begin{array}{l} k \leftarrow \text{Gen}() \\ \text{Enc}(k, m_2) \end{array} \right\}$$

$k = c' \oplus m$

$m_1 \oplus k$

$m_2 \oplus k$

$$\forall m, c'. \Pr\left[\begin{array}{c} k \leftarrow \text{Gen} \\ c \leftarrow \text{Enc}(k,m) \\ \hline c = c' \end{array} \right] = \frac{1}{|\mathcal{M}|}$$

Let (Enc, Gen, Dec) be a Uniform ciphertext scheme
correct scheme...

Construct Enc', Gen', Dec'' that is correct, perfect secret,
but NOT uniform

$$Enc'(k, m) = c \leftarrow Enc(k, m)$$

return $c' = 0 \cdot c$

$M = [0 \ldots 2^n]$

$C' = \{0,1\} \times C$

$C = [0 \ldots 2^n + 2^n]$

Shannon's secrecy:

"even with prior information about m,
c gives no additional information"

posterior

$$\forall \mathcal{D}, c', m'. \ \Pr\left[\begin{array}{c} m \leftarrow \mathcal{D} \\ k \leftarrow Gen \\ c \leftarrow Enc(k,m) \\ \hline m = m' \end{array} \,\middle|\, c = c' \right] =$$

$$\Pr\left[\begin{array}{c} m \leftarrow \mathcal{D} \\ \hline m = m' \end{array}\right]$$

For next time: Q 1.1 from Joy

Suppose Uniform Ciphertexts holds

arbitrary

for (Enc, Dec, Gen). And we

encrypt the same message m twice (using fresh keys)?

Is this secure?