Modern Cryptography

Private Key Encryption Scheme

Shashank Singh

IISER Bhopal

Private Key Encryption-updated defnition

It is defined by three algorithms $(\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$, and a specification of a finite message space $\mathcal{M}$, with $|\mathcal{M}| > 1$, with the follwoing properties:

GEN: $k \leftarrow \texttt{GEN}()$, a probabilistic algorithm that outputs a key k. $\mathcal{K} = \{k \mid k \leftarrow \texttt{GEN}()\}$ is the key space.

ENC: A probabilistic algorithm ENC. $c \leftarrow \texttt{ENC}(k, m)$ where $k \in \mathcal{K}$ and $m \in \mathcal{M}$. We denote by $\mathcal{C} = \{\texttt{ENC}_r(k, m) : k \in \mathcal{K}, m \in \mathcal{M}$ and r is randomness of $\texttt{ENC}\}$

DEC: It is the decryption algorithm. $m := \texttt{DEC}(k, c)$ where $k \in \mathcal{K}$ and $c \in \mathcal{C}$.

Furthermore, $\texttt{DEC}_k\left(\texttt{ENC}_k\left(m\right)\right) = m \forall m \in \mathcal{M}, \forall k \in \mathcal{K}$.

Private-key Encryption -modified definition

It is a tuple of PPT algorithms $(\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$, such that

- The key-generation algorithm $\texttt{GEN}$ takes input as 1^n and outputs a key k; we write $k \rightarrow \texttt{GEN}(1^n)$.
(wlog assume $|k| > n \quad \forall k$)
- $c \leftarrow \texttt{ENC}(k, m)$ where $m \in \{0,1\}^*$.
- The decryption algorithm $\texttt{DEC}$ takes as input a key k and a ciphertext c, and outputs a message m or an *error*.

It is required that for every n, for every key k output by $\texttt{GEN}(1^n)$ and every $m \in \{0,1\}^*$, it holds that $\texttt{DEC}(k, \texttt{ENC}(k, m)) = m$.

- We denote by $\mathbf{K}$ a random variable denoting the value of the key output by `GEN`, thus for any $k \in \mathcal{K}$, $\Pr[\mathbf{K} = k]$ denotes the probability that the key output by `GEN` is equal to k.
- Similarly $\mathbf{M}$ and $\mathbf{C}$ will be used to represent the random variable for message space and key space.
- Furthermore $\mathbf{K}$ and $\mathbf{M}$ are assumed to be independent.

Example

Consider a Shift Cipher. We have $\mathcal{K} = \{0, 1, 2, \ldots, 25\}$ with $\Pr[\mathbf{K} = k] = 1/26$ for each $k \in \mathcal{K}$. Assume that we are give the following distribution over $\mathcal{M}$.

$$\Pr[M = y] = 0.7 \text{ and } \Pr[M = n] = 0.3$$

What is the probability that the ciphertext is B?

PERFECT SECRECY

Definition

An encryption scheme $(\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ with message space $\mathcal{M}$ is perfectly secret if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ for witch $\Pr[\mathbf{C} = c] > 0$;

$$\Pr[\mathbf{M} = m | \mathbf{C} = c] = \Pr[\mathbf{M} = m] \tag{1}$$

EXERCISE:

An encryption scheme $(\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ with message space $\mathcal{M}$ is perfectly secret if and only if the following holds for every $m, m' \in \mathcal{M}$:

$$\Pr\left[\texttt{ENC}\left(m\right) = c\right] = \Pr\left[\texttt{ENC}\left(m'\right) = c\right], \tag{2}$$

where the probabilities are over choice of key k and internal randomness of $\texttt{ENC}$.

Note that,

- $\Pr\left[\texttt{ENC}(m) = c\right] = \Pr\left[\mathbf{C} = c \mid \mathbf{M} = m\right]$
- The Eq. 2 implies that $\Pr\left[\mathbf{C} = c \mid \mathbf{M} = m\right]$ is independent of m.
- The set $\{\Pr\left[\mathbf{C} = c \mid \mathbf{M} = m^\star\right] : c \in \mathcal{C}\}$ is the distribution of cipher text when the message $m^\star$ is encrypted.

SOLUTION:

Eqn. 1 $\Longleftarrow$ **Eqn. 2**

– Let $\Pr[\mathbf{C} = c] > 0$, by the law of total probability

$$
\begin{aligned}
\Pr[\mathbf{C} = c] &= \sum_{m \in \mathcal{M}} \Pr[\mathbf{C} = c \mid \mathbf{M} = m] \cdot \Pr[\mathbf{M} = m] \\
&= \sum_{m \in \mathcal{M}} \Pr[\textsc{Enc}(m) = c] \cdot \Pr[\mathbf{M} = m] \\
&= \Pr[\textsc{Enc}(m) = c] \cancelto{1}{\sum_{m \in \mathcal{M}} \cdot \Pr[\mathbf{M} = m]}.
\end{aligned}
$$

Hence, $\Pr[\mathbf{M} = m \mid \mathbf{C} = c] = \Pr[\mathbf{M} = m]$. (By Bayes' Rule)

Eqn. 1 $\implies$ Eqn. 2

We will prove the contrapositive. $\neg$Eqn. 2 $\implies$ $\neg$Eqn. 1.

- Let $q = \Pr[\mathbf{C} = c \mid \mathbf{M} = m]$ and $q' = \Pr[\mathbf{C} = c \mid \mathbf{M} = m']$. WLOG, we can assume $q > q'$.
- Consider a distribution on $\mathcal{M}$ with support $\{m, m'\}$. Let $\Pr[\mathbf{M} = m] = p$, $\Pr[\mathbf{M} = m'] = 1 - p$.
- $\Pr[\mathbf{C} = c] = q \cdot p + q' \cdot (1 - p)$, hence $q' < \Pr[\mathbf{C} = c] < q$.
- $\Pr[\mathbf{M} = m \mid \mathbf{C} = c] = \left(\frac{q}{q \cdot p + q' \cdot (1-p)}\right) \cdot p > p$; a contradiction!

Perfect Indistinguishability

Let $\Pi = (\mathtt{GEN}, \mathtt{ENC}, \mathtt{DEC})$ be an encryption scheme with message space $\mathcal{M}$. For an adv. $\mathcal{A}$, we define an experiment as follows:

$\mathrm{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi}$:

1. $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.
2. A key $k \leftarrow \mathtt{GEN}()$ and $b \xleftarrow{\$} \{0,1\}$ are chosen. The challenge ciphertext $c \rightarrow \mathtt{ENC}_k(m_b)$ is given to $\mathcal{A}$.
3. $\mathcal{A}$ outputs a bit b'.
4. The experiment returns $b' \stackrel{?}{=} b$.

If $\mathrm{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi} = 1$, we say that the adv. $\mathcal{A}$ succeeds.

Perfect Indistinguishability..

Definition

An encryption scheme $\Pi = (\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ with message space $\mathcal{M}$ is perfectly indistinguishable if for every $\mathcal{A}$ it holds that

$$\Pr\left[\mathrm{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}$$

HOMEWORK

Exercise: An encryption scheme Π is perfectly secret if and only if it is perfectly indistinguishable

SOLUTION: PI $\implies$ PS

We prove $\neg$PS $\implies$ $\neg$PI.

- There exists $m_0, m_1 \in \mathcal{M}$ and $c \in \mathcal{C}$ such that

$$\underbrace{\Pr\left[\mathbf{C} = c \mid \mathbf{M} = m_0\right]}_{q_0} \neq \underbrace{\Pr\left[\mathbf{C} = c \mid \mathbf{M} = m_1\right]}_{q_1}.$$

- WLOG, we can assume $q_0 > q_1$. We construct an adversary $\mathcal{A}$ for which, $\Pr\left[\mathrm{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] > \frac{1}{2}$.
  - $\mathcal{A}(c') = 0$ if $c' = c$; 1 otherwise.
-

$$\begin{aligned}\Pr\left[b' = b\right] &= \frac{1}{2}\Pr\left[b' = 0 \mid b = 0\right] + \frac{1}{2}\Pr\left[b' = 1 \mid b = 1\right] \\ &= \frac{1}{2}q_0 + \frac{1}{2}(1 - q_1) = \frac{1}{2} + \frac{1}{2}(q_0 - q_1) > \frac{1}{2}\end{aligned}$$

Solution: PS $\implies$ PI

- $\mathcal{A}$'s behavior $b' := \mathcal{A}(c)$ depends only on c and not on b as the distribution of the input c remains the same irrespective of $b = 0$ or $b = 1$. (Def. of Perfect Secracy)
- Let $\Pr\left[b' = 1 \mid b = 0\right] = \Pr\left[b' = 1 \mid b = 1\right] = p$ (say) .
- $$\begin{aligned} \Pr\left[b' = b\right] &= \frac{1}{2}\,\Pr\left[b' = 0 \mid b = 0\right] + \frac{1}{2}\,\Pr\left[b' = 1 \mid b = 1\right] \\ &= \frac{1}{2}\,(1 - p) + \frac{1}{2}\,p = \frac{1}{2} \end{aligned}$$

Vernam Cipher (One Time Pad)

Definition

Fix an integer $\ell > 0$. The message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$ are all equal to $\{0,1\}^\ell$.

- $\texttt{GEN}$ chooses the key k according to uniform distribution on $\mathcal{K}$.
- Given a key $k \in \{0,1\}^\ell$ and a message $m \in \{0,1\}^\ell$,

$$\texttt{ENC}_k(m) = m \oplus k$$

- Given a key $k \in \{0,1\}^\ell$ and a ciphertext $c \in \{0,1\}^\ell$,

$$\texttt{DEC}_k(c) = c \oplus k$$

Exercise: One-time pad encryption scheme is perfectly secret.

VERNAM CIPHER (ONE TIME PAD)

Definition

Fix an integer $\ell > 0$. The message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$ are all equal to $\{0,1\}^\ell$.

- GEN chooses the key k according to uniform distribution on $\mathcal{K}$.
- Given a key $k \in \{0,1\}^\ell$ and a message $m \in \{0,1\}^\ell$,

$$\texttt{ENC}_k(m) = m \oplus k$$

- Given a key $k \in \{0,1\}^\ell$ and a ciphertext $c \in \{0,1\}^\ell$,

$$\texttt{DEC}_k(c) = c \oplus k$$

Exercise: One-time pad encryption scheme is perfectly secret.

Theorem

One-time pad encryption scheme is perfectly secret.

Proof.

... $\square$

Theorem

If $(\texttt{GEN}, \texttt{ENC}, \texttt{DEC})$ *is a perfectly secret encryption scheme with message space* $\mathcal{M}$ *and key space* $\mathcal{K}$*, then* $|\mathcal{K}| \geq |\mathcal{M}|$*.*

Proof.

... $\square$