Fix a distribution over $\mathcal{M}$, a message m and a ciphertext c for which $\Pr[C=c] > 0$.

We have to show that given

$$\Pr[Enc_k(m) = c] = \Pr[Enc_k(m') = c] \quad \forall m, m' \in \mathcal{M} \text{ and } \forall c \in \mathcal{C}$$

$$\Rightarrow \Pr[M = m \mid C = c] = \Pr[M = m]$$

If $\Pr[M=m] = 0$ then trivially we have the above relation.

Assume $\Pr[M = m] > 0$.

We have $\Pr[C = c \mid M = m]$

the entire space

$$= \Pr[Enc_k(M) = c \mid M = m]$$

$$= \Pr[Enc_k(m) = c]$$

(The first equality by the definition of R.V. C and second because we are conditioning on m.

Let $p = \Pr[Enc_K(m) = c]$

$= \Pr[C = c \mid M = m]$

We have $\forall m' \in \mathcal{M}$ we have

$\Pr[Enc_K(m') = c]$

$= \Pr[C = c \mid M = m'] = p$

$$\Pr[M = m \mid C = c] = \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\Pr[C = c]}$$

$$= \frac{\Pr[C = c \mid M = m] \cdot \Pr[M = m]}{\sum_{m' \in \mathcal{M}} \Pr[C = c \mid M = m'] \cdot \Pr[M = m']}$$

$$= \frac{p \cdot \Pr[M = m]}{\sum_{m' \in \mathcal{M}} p \cdot \Pr[M = m']}$$

$$= \Pr[M = m].$$

So scheme is perfectly secret.

$\Rightarrow$ Given that a scheme is perfectly secret

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

$$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$$

T.S.T. $\Pr[\mathrm{Enc}_k(m) = c] = \Pr[\mathrm{Enc}_k(m') = c]$

$$\forall m, m' \in \mathcal{M}$$

i.e. T.S.T. $\Pr[C = c \mid M = m] = \Pr[C = c \mid M = m']$

$$\Pr[C=c \mid M=m] = \frac{\Pr[M=m \mid C=c] \cdot \Pr[C=c]}{\Pr[M=m]}$$

$$= \frac{\Pr[M=m] \cdot \Pr[C=c]}{\Pr[M=m]}$$

$$= \Pr[C=c]$$

$$\Pr[C=c \mid M=m'] = \frac{\Pr[M=m' \mid C=c] \cdot \Pr[C=c]}{\Pr[M=m']}$$

$$= \Pr[C=c]$$

Perfect (adversarial) indistinguishability is slightly different but also gives another equivalent definition of perfect secrecy.

very common to define security in crypto

This definition is based on an $\boxed{\text{experiment}}$ involving an adversary passively observing a ciphertext and then trying to guess which two possible messages are encrypted.

<u>Experiment</u>: An adversary $\mathcal{A}$ first specifies two arbitrary messages $m_0, m_1 \in \mathcal{M}$.

→ One of these two messages is chosen uniformly at random and encrypted using a random key.

→ The resulting ciphertext is given to $\mathcal{A}$.

→ $\mathcal{A}$ outputs a "guess" as to which of the two messages was encrypted.

→ $\mathcal{A}$ succeeds if it guesses correctly.

→ An encryption scheme is perfectly indistinguishable if no adversary $\mathcal{A}$ can succeed with probability better than $1/2$

(note that $\mathcal{A}$ can succeed with probability $1/2$ by outputting a uniform guess. The requirement here is that an attacker cannot do better than this).

Formal description:

Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$.

Let $\mathcal{A}$ be an adversary,

formally it is a stateful algorithm.

$\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$ (adversarial indistinguishability exp)

1. $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.

2. A key k is generated using Gen, and a uniform bit $b \in \{0,1\}$ is chosen.

3. $c \leftarrow Enc_k(m_b)$ is computed and given to $\mathcal{A}$.

challenge ciphertext

4. $\mathcal{A}$ outputs a bit b'.

5. Output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

We write $PrivK^{eav}_{\mathcal{A},\Pi} = 1$ if the o/p of the exp is 1 and

we say that $\mathcal{A}$ succeeds.

<u>Def</u>: Encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ is perfectly indistinguishable if for every $\mathcal{A}$ it holds that

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

<u>Lemma</u>: Encryption scheme Π is perfectly secret iff it is perfectly indistinguishable.

Proof:

Perfectly secret $\Rightarrow$ perfectly indistinguishable.

Fix $\mathcal{A}$ and m_0, m_1 output by $\mathcal{A}$. We know from the equivalent definition of perfect secrecy,

$$\Pr[\mathrm{Enc}_k(m_0) = c]$$
$$= \Pr[\mathrm{Enc}_k(m_1) = c].$$

Let C_0 (resp. C_1) denote the set of ciphertext for which $\mathcal{A}$ outputs 0 (resp. 1)

at the conclusion of $PrivK^{eav}_{\mathcal{A},\Pi}$.
We have set of all ciphertexts C,
$C = C_0 \cup C_1$

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

This is experiment output 1 and not $\mathcal{A}$ outputting 1.

$$= \frac{1}{2} \cdot \Pr[\mathcal{A} \text{ outputs } 0 \mid b = 0]$$
$$+ \frac{1}{2} \cdot \Pr[\mathcal{A} \text{ outputs } 1 \mid b = 1]$$

$$= \frac{1}{2} \sum_{c \in C_0} \Pr[c = Enc_k(m_0)]$$
$$+ \frac{1}{2} \sum_{c \in C_1} \Pr[c = Enc_k(m_1)]$$

$$= \frac{1}{2} \sum_{c \in C_0} \Pr\left[c = Enc_k(m_0)\right]$$

$$+ \frac{1}{2} \sum_{c \in C_1} \Pr\left[c = Enc_k(m_0)\right]$$

$\because Enc_k(m_0) = Enc_k(m_1)$

$$= \frac{1}{2} \sum_{c \in C} \Pr\left[c = Enc_k(m_0)\right]$$

$$= \frac{1}{2}.$$

Now for the opposite direction: given that we have perfectly indistinguishable encryption scheme, to show that

it is perfectly secret.

We prove the contrapositive:

Assume Π is not perfectly secret.

$\Rightarrow \exists\, m_0, m_1 \in \mathcal{M}$ and $c' \in \mathcal{C}$

s.t. $\Pr[\mathrm{Enc}_k(m_0) = c'] \neq \Pr[\mathrm{Enc}_k(m_1) = c']$

Let $\mathcal{A}$ output m_0, m_1 in the first step of $\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi}$.

$\rightarrow$ Then if $\mathcal{A}$ receives any ciphertext $c'' \neq c'$ then it outputs a uniform bit b'.

If it receives c' it outputs $b' = 0$.

Since each is chosen with probability $1/2$, we have:

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

$$= \frac{1}{2} \cdot \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 \mid M = m_0\right]$$

$$+ \frac{1}{2} \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 \mid M = m_1\right]$$

Lets look at

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 \mid M = m_0\right]$$

$$= \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 \wedge c' = \mathrm{Enc}_k(m_0)\right]$$

$$+ \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 \wedge c' \neq \mathrm{Enc}_k(m_0)\right]$$

$$= \Pr\left[c' = \mathrm{Enc}_k(m_0)\right] + \frac{1}{2}\Pr\left[c' \neq \mathrm{Enc}_k(m_0)\right]$$

since if its c' then A will also output $b'=0$. so always 1.

Now when $M = m_1$.

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{A,\Pi} = 1 \,/\, M = m_1\right]$$

$$= \frac{1}{2} \cdot \Pr\left[c' \neq \mathrm{Enc}_k(m_1)\right]$$

$$\left[\because \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{A,\Pi} = 1 \wedge c' = \mathrm{Enc}_k(m_1)\right] = 0\right]$$

Putting all together we get

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

$$\frac{1}{2}\cdot\Big(\Pr\left[c' = \mathrm{Enc}_k(m_0)\right] + \frac{1}{2}\Pr\left[c' \neq \mathrm{Enc}_k(m_0)\right]\Big) + \frac{1}{2}\cdot\frac{1}{2}\cdot\Pr\left[c' \neq \mathrm{Enc}_k(m_1)\right]$$

$$= \frac{1}{2}\cdot\Big(\Pr\left[c' = \mathrm{Enc}_k(m_0)\right] + \frac{1}{2}\left(1 - \Pr\left[c' = \mathrm{Enc}_k(m_0)\right]\right)\Big) + \frac{1}{4}\cdot\Pr\left[c' \neq \mathrm{Enc}_k(m_1)\right]$$

$$= \frac{1}{4} + \frac{1}{4} \cdot \Pr\left[c' = Enc_k(m_0)\right]$$

$$+ \frac{1}{4} \cdot \Pr\left[c' \neq Enc_k(m_1)\right]$$

$$\neq \frac{1}{4} + \frac{1}{4} \cdot \Pr\left[c' = Enc_k(m_1)\right]$$

$$+ \frac{1}{4} \cdot \Pr\left[c' \neq Enc_k(m_1)\right]$$

$$= \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

Since $\Pr\left[PrivK^{cpa}_{A,\Pi} = 1\right] \neq 1/2$

$\Rightarrow$ not perfectly indistinguishable.