Given message independence:

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

Prove ciphertext independence:

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

Using conditional probability

$$Pr[C=c] = \Sigma_K Pr[C=c \mid K=k] \cdot Pr[K=k]$$

applying Bayes theorem:

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

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

thus

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

following

$$Pr[C=c \mid M=m_1] = Pr[C=c \mid M=m_2]$$

Thus proving ciphertext is independent of the message text.

$A \Leftrightarrow B$

$A \longrightarrow B$

C D

Following the previously given ciphertext :

$Pr[C=c \mid M=m_1] = Pr[C=c \mid M=m_2] = Pr[C=c]$

Prove Perfect adversarial indistinguishability :

$Pr[\text{priv}K^{eav}_{A,\Pi} = 1] = 1/2$

$C = Enc_K(m_b)$

$b \in \{0,1\}$ given two messages

causing,

$Pr[b' = b] = 1/2$

$\frac{1}{2} = Pr[\text{priv}K^{eav}_{A,\Pi} = 1]$

$\Rightarrow Pr[C=c \mid M=m_1] \cdot Pr[M=m_1] +$
$Pr[C=c \mid M=m_2] \cdot Pr[M=m_2] \Rightarrow$

$Pr[b'=b] = Pr[b'=b \mid b=0] \cdot Pr[b=0] +$
$Pr[b'=b \mid b=1] \cdot Pr[b=1]$

$Pr[b'=b] = ((1/2)(1/2)) + ((1/2)(1/2))$

$Pr[b'=b] = (1/4) + (1/4)$
$= 2/4 = 1/2 = Pr[\text{priv}K^{eav}_{A,\Pi} = 1]$

Thus,

An adversary cannot distinguish between two encrypted messages better than random guessing.

$$\begin{tikzcd} A \arrow[r] & B \arrow[dl] \\ C & D \end{tikzcd}$$

Given: P.A.I

$Pr[PrivK^{eav}_{A,\pi} = 1] = 1/2$

Prove perfect secrecy:

$$Pr[enc(k, m_1) = c_1] = Pr[enc(k, m_2) = c]$$
$$= Pr[C = c \mid M = m_1] = Pr[C = c \mid M = m_2]$$

$$Pr[PrivK^{eav}_{A,\pi} = 1] = \left.\begin{array}{l} \overbrace{Pr[C = c \mid M = m_1] \cdot Pr[M = m_1]}^{b=0} + \\ \underbrace{Pr[C = c \mid M = m_2] \cdot Pr[M = m_2]}_{b=1} = \end{array}\right\} 1/2$$

$$\Rightarrow Pr[C = c \mid M = m_1] \cdot 1/2 + Pr[C = c \mid M = m_2] \cdot 1/2$$

Since $Pr[b' = b] = 1/2$

$$\Rightarrow Pr[C = c \mid M = m_1 = C = c \mid M = m_2] = 1/2$$

thus,

$$(Pr[enc(k, m_1) = c] = Pr[enc(k, m_2) = c]) = 1/2$$

being adversary having no advantage as both messages have a 1/2 probability following P.A.I.
proving perfect secrecy is equivalent to P.A.I.

$$\begin{tikzcd} A \arrow[r] & B \arrow[dl] \\ C \arrow[r] & D \end{tikzcd}$$

E

Given perfect secrecy:

$$Pr[C=c \mid M=m_1] = Pr[C=c \mid M=m_2] = Pr[C=c]$$

Prove message independance

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

again, substituting bayes Theorem:

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

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

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

thus,

not only showing perfect serecy is equivulent to message independence, but also equivalent to cipher independence, as we applied that definition also.

$$\begin{tikzcd}
A \arrow[r] & B \arrow[d] \arrow[dl] \\
C \arrow[r] & D \arrow[ul]
\end{tikzcd}$$

Extra unrelated notes!!!!:

Reflexive
Symmetric
Transitive
equivalent

OTP

og txt + key padtxt = ctxt
ello ubv; 1'.@T

Assume Perfect Secrecy:

Perfect secrecy is the condition where the probability distribution of a message $M=m$ given a ciphertext $C=c$ is independent of the ciphertext. This means the ciphertext reveals no information about the message.

$$Pr[enc(k, m_0) = C] = Pr[enc(k, m_1) = C]$$

where $\forall m \in M$, $\forall c \in C$ where $Pr[C=c] > 0$

Message independence (Shannon Secrecy)

we want to show:

$Pr[M=m \mid C=c] = Pr[M=m]$, ciphertext proves no information about the message, therefore M and C must be independent. The encryption algorithm generates cipher text uniformally (of equal distribution).

$$Pr(C=c) = \Sigma_k Pr[C=c \cap K=k]$$

$$\begin{aligned} Pr[C=c \cap K=k] &= Pr[M=c+k \cap K=k] \\ &= Pr[M=c+k] \, P[K=k] \\ &= Pr[M=c+k] \, (1/N) \end{aligned}$$

we know k runs through all possible keys, $c+k$ runs through all possible messages

$$\Sigma_k Pr[M=c+k] = Pr[M = \text{some possible message}] = 1$$ Why

therefore,

$$Pr[C=c] = \Sigma_k Pr[C=c \cap K=k] = (1/N) \Sigma_k Pr[M = c+k] = 1/N$$

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

$\therefore \; Pr[M=m \mid C=c] = \dfrac{Pr[C=c \mid M=m]\,Pr[M=m]}{Pr[C=c]}.$

$\cancel{\frac{1}{Pr}} \; Pr[C=c] \cdot Pr[\cancel{M}=m] = \dfrac{Pr[C=c \mid M=m]\,Pr[\cancel{M=m}]}{Pr[\cancel{C=c}]} \cdot \dfrac{1}{\cancel{Pr[M=m]}} \cdot \cancel{Pr[C=c]}$

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

$\Rightarrow \; Pr[C=c] = Pr[C=c]\,Pr[M=m]$

$1 = Pr[M=m]$

C: $Pr[C=c \mid M=m] = \dfrac{1}{|C|}$

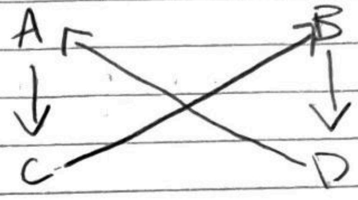
$Pr[C=c] = \dfrac{1}{|C|} Pr[M=m]$

$Pr[C=c] = \dfrac{1}{|C|} \sum_{m \in M} Pr[M=m]$

$\cup$ unison
$\cap$ intersection

WTS: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

set $A = \{1, 2, 3\}$
set $B = \{2, 3, 4\}$
set $C = \{3, 4, 5\}$



A: $(A \cup B) \cap C$:
$(A \cup B) = \{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\}$
B: $(A \cup B) \cap C = \{1,2,3,4\} \cap \{3,4,5\} = \{3,4\}$

$(A \cap C) = \{3\}$
$(B \cap C) = \{3,4\}$
$(A \cap C) \cup (B \cap C) = \{3\} \cup \{3,4\} = \{3,4\}$

$(A \cap B$