Eavesdropping Adversary Attack Prevention

An Eavesdropping Adversary listens to the channel and has access to only the ciphertext. They can perform reverse engineering, frequency analysis, etc. on the ciphertexts collected if the ciphertext reflects any property of the original message.

In this case, we encrypt the message m as follows:

$$c = Enc_K(m) = G(k) \oplus m$$

where G is a pseudo-random generator.
The ciphertext c is sent via the channel.
Here, k is a uniformly sampled key known only to sender and receiver.

For decryption,

$$Dec_K(c) = c \oplus G(k) = G(k) \oplus m \oplus G(k)$$
$$= m$$

Let U_n denote a n-bit string ~~value~~ sampled from uniform distribution over n-bit strings where n is the length of the key k. From the definition of pseudo-random generator, $\forall$ PPTM adversary A,

$$\left| P[A(U_{len(m)}) = 1] - P[A(G(U_n)) = 1] \right| \le negl(n)$$

$$\Rightarrow \left| P[A(U_{len(m)}) = 1] - P[A(G(k)) = 1] \right| \le negl(n)$$

Let k' be a uniformly sampled len(m) −bit string.

Hence,

$$\left| P\left[A(k')=1\right] - P\left[A(G(k))=1\right] \right| \leq negl(n)$$

Let us take the encryption scheme,

$$c = k' \oplus m$$

$$P(c|m_0) = P(c = m_0 \oplus k') = P(k' = c \oplus m_0)$$

$$P(c|m_1) = P(c = m_1 \oplus k') = P(k' = c \oplus m_1)$$

for messages m_0 and m_1.

Since k' is selected at random from the uniform distribution,

$$P(k' = c \oplus m_0) = P(k' = c \oplus m_1)$$

$$\Rightarrow P(c|m_0) = P(c|m_1)$$

Which follows Shannon's definition of perfect security. Hence, our original encryption scheme deviates from perfect security by negl(n). It satisfies perfect security with the relaxations of PPTM adversary and negl(n) error bound.

Scanned with OKEN Scanner