Eavesdropping Adversary

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 some known property of the original message.
In this case, we encrypt the message m as follows:

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

We send c through the channel. Here, k is a uniformly sampled secret key known to only the sender and receiver. G is a pseudo-random generator. For decryption,

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

Let U_n denote the 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,

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

$$\implies |P[A(U_{len(m)}) = 1] - P[A(G(k)) = 1]| \leq negl(n)$$

Let $k' \in U_{len(m)}$. Hence,

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

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 distinct messages m_0 and m_1.
Since k' is sampled from uniform distribution,

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

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

which follows Shannon's definition of perfect security. This is also called one-time pad. Hence, our original encryption scheme negligibly deviates from perfectly secure one-time pad which satisifes perfect security definition with relaxed conditions.