Pseudo-random Function

A function F : {0, 1}^k x {0, 1}^* -> {0, 1}^n is a Pseudo-random function (PRF) if, for any probabilistic polynomial-time (PPT) adversary A, the advantage of A in distinguishing F from a truly random function is negligible.

Proof of security of Pseudo-random function

1. Suppose we have a cryptographic scheme that uses a PRF F for encryption.
2. Let's suppose there exists an efficient adversary A that can break the security of the scheme, that is, A can distinguish the encrypted messages produced by the scheme from random strings with non-negligible advantage.
3. We can use A to construct a distinguisher D that can distinguish F from a truly random function with non-negligible advantage.
4. Here's how D works: - Given an input (k, x), D selects a random bit b and constructs a ciphertext by computing C = Enc_k(x) XOR (b || F (k, x)), where || denotes concatenation.
5. D sends the ciphertext C to A, who must guess the value of b. If A correctly guesses b with probability greater than 1/2 + epsilon, then D outputs 1, indicating that F is not a PRF. Otherwise, D outputs 0.
6. We can show that the advantage of D in distinguishing F from a truly random function is equal to the advantage of A in breaking the security of the scheme, which we know to be non-negligible.
7. This is a contradiction, as we assumed that F is a PRF and that no efficient adversary can distinguish it from a truly random function with non-negligible advantage.

8. Therefore, the scheme that uses **F as a PRF for encryption is secure.**