PRF from PRG.

Construction of PRF from PRG:-

Let G be a pseudorandom generator with expansion factor $l(n) = 2n$. Denote by $G_0(k)$ the first half of G's output, and by $G_1(k)$ the second half of G's output. For every $k \in \{0,1\}^n$, define the function $F_k : \{0,1\}^n \to \{0,1\}^n$ as:

$$F_k(x_1, x_2, x_3 \ldots x_n) = G_{x_n}(\ldots(G_{x_2}(G_{x_1}(k)))\ldots)$$

Theorem: If G is a pseudorandom generator with expansion factor $l(n) = 2n$, then the above function is a PRF.

PRF

→ we have to build a Pseudorandom function such that even if the other party gets the encryption key they should not be able to decrypt and study what's the content is about.
Server for that session

for this we take probabilistic algorithm instead of using a deterministic algorithm.

Pseudorandom function F_k

encrypt r and add to it

So the basic idea to generate $c = (r, F_k(r) \oplus m)$
so that decryption is easy

functions should be easy to compute, Computationally the function should be identical to random function, say from domain $\{0,1\}^n$ to co-domain $\{0,1\}^n$

→ There are 2^{n2^n} possible functions so the CPA is not possible in this kind of probablistic algorithm.

DEF let $F: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient, length-preserving, keyed function. We say that F is a Pseudorandom function if for all probablistic polynomial-time distinguishers D, there exists a negligible function negl such that:

$$\left| \Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \right| \leq negl(n);$$

Where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from the set of functions mapping n-bit strings to n-bit strings.