Cryptology: Problem Sheet 2

Nilanjan Datta

IAI, TCG CREST

1. Say CBC-mode encryption is used with a 128-bit PRF having a 256-bit key to encrypt a 1024-bit message. What is the length of the resulting ciphertext?

2. How do you encrypt a 520-bit message using CBC, OFB and CTR mode using an 128-bit PRF?

3. Let F be a secure PRF defined over $(\{0,1\}^n, \{0,1\}^n, \{0,1\}^n)$.

   (a) Prove that $G_k(x, y) := F_k(x) \oplus F_k(y)$ is not a secure PRF.

   (b) Prove that $G_k(x) := F_k(x) \oplus F_k(x \oplus 1^n)$ is not a secure PRF.

4. Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. In each of the following cases, say whether G' is a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

   (a) Define $G'(s) = G(s_1 \cdots s_{n/2})$, where $s = s_1 \cdots s_n$.

   (b) Define $G'(s) = G(0^{|s|} \| s)$.

   (c) Define $G'(s) = G(s) \| G(s + 1)$.

5. Let F be a pseudorandom function mapping 128-bits to 128-bits. Consider the mode of operation in which a uniform value $r \leftarrow_\$ \{0,1\}^{64}$ is chosen, and the i-th ciphertext block c_i is computed as

   $$c_i := F_k(r \| i) \oplus m_i.$$

   What is the maximum message length that can be encrypted using this scheme? Does this scheme have indistinguishable encryptions in the presence of an eavesdropper.