

CSE 408/508 Fall 2009: Homework #1

CSE 508 Students: Solve 3 of the following problems.

CSE 408 Students: Solve 2 of the following problems.

Problem 1

Suppose $G : \{0, 1\}^\ell \rightarrow \{0, 1\}^L$ is a secure PRG (for some values of (t, ϵ)). For each of the following constructions, say whether it is always a secure PRG or not. Include a proof or counterexample for your answer.

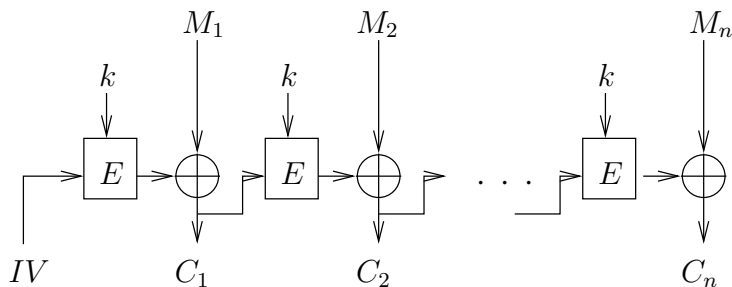
- $G'(x) = G(x) || G(x)$
- $G'(x) = G(x) || f(G(x))$, where f is any polynomial-time function.
- $G'(x) = G(x) || G(x + 1)$
- $G'(x) = G(f(x))$, where f is any polynomial-time function.

Problem 2

Prove the fact we used in class: if $X \leftarrow U_\ell$ and $Y \leftarrow D$, where D is any distribution on $\{0, 1\}^\ell$, then $X \oplus Y$ is uniformly distributed.

Problem 3

In CFB mode, diagrammed below, the IV is incremented for each message.



Prove that, if E is a (t, q, ϵ) -secure PRF, then CFB^E is $(t - O(q), \min(q, |\text{Ctrs}|), \epsilon)$ R-or-R secure.

Problem 4

One intuitive definition of security for an encryption algorithm is that its ciphertexts should “look random.” We can formalize this idea as follows:

Definition An encryption scheme E is (t, q, ϵ) RC-secure (“randomness of ciphertexts”) if

- For all k, k', x, y such that $|x| = |y|$, $|E(k, x)| = |E(k', y)|$. In other words, the length of E ’s ciphertext only depends on the length of the plaintext.
- For all adversaries A running in time t and making q oracle queries,

$$\text{Adv}_A = |\Pr[A^{E_k} = 1] - \Pr[A^{S \circ E_k} = 1]| \leq \epsilon$$

Prove that RC-security implies IND-CPA security.
(Fact: IND-CPA does not imply RC-security.)

Problem 5

In CBC mode, the IV is chosen randomly for each message. Suppose that instead, we increment the IV for each message, i.e. the first message uses an IV of 0, the second message uses an IV of 1, etc. Show that this CBC variant is not IND-CPA secure. In other words, describe an adversary that can break this scheme using a small number of plaintext queries and a small amount of computation.