

CSE 690: Problem Set #2

Problem 1: Randomness of Ciphertexts

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 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,

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

Prove that RC-security implies IND-CPA security (you may use any version of IND-CPA security), but that IND-CPA does not imply RC-security.

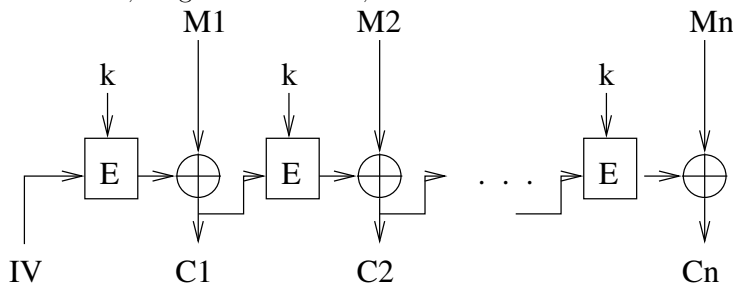
Problem 2: CBC IVs

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.

Generalize the above attack. Suppose the attacker can predict the IV that will be used for each message with probability p . How quickly can you IND-CPA break this version of CBC mode?

Problem 3: Cipher Feedback Mode

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: Design a Block Cipher

Design a block cipher $E : \{0, 1\}^l \times \{0, 1\}^n \rightarrow \{0, 1\}^n$. Specify the key size, l , and block size, n , and give a concise description of the algorithm for encryption. You do not have to describe or prove that your cipher is invertible, but you should double-check that it is before turning it in. Your description should fit on one side of one page of paper. Diagrams are encouraged.

Grading will be based on simplicity, security, and performance.