

Take-home Midterm Exam

Due *start of* class Monday, April 14, 2008.

Instructions: Please start each problem on a new page and leave a blank line or two between subparts. You may type or hand write your solutions, but they should be legible, concise, and answer all parts of each question. Do not discuss the exam with anyone in or outside of the class. You may use any of the resources listed on the course home page (BR notes, HAC, Modern Cryptography book, solutions I've posted) as well as your class notes. You are also free to use any of the various books I have in my office. If you think you need any additional resources, please check with me first before consulting them.

Problem 1. [15 points] As we have seen, the definition of indistinguishability against chosen plaintext attack for symmetric encryption (IND-CPA) described in the Bellare, Rogaway notes uses a “left-right” encryption oracle $\text{Enc}_K(\text{LR}(\cdot, \cdot, b))$. Consequently, this is known as the left-right definition of IND-CPA. Another, equivalent way to model chosen plaintext attack, which I'll denote CPA2, uses a plain encryption oracle $\text{Enc}_K(\cdot)$ at the expense of a slightly more complicated experiment. In the security experiment below, A is a “stateful” which means it “remembers” everything it did¹ prior to receiving “challenge ciphertext” c .

Experiment $\text{Exp}_A^{\text{IND-CPA2-b}}$

```

 $K \xleftarrow{\$} \text{Gen}()$ 
 $(m_1, m_2) \leftarrow A^{\text{Enc}_K(\cdot)}$ 
 $c \leftarrow \text{Enc}_K(m_b)$ 
 $b' \leftarrow A^{\text{Enc}_K(\cdot)}(c)$ 
return  $b'$ 

```

The definition of advantage is the same, namely

$$\text{Adv}_{\text{SE}}^{\text{ind-cpa2}}(A) = \Pr[\text{Exp}_{\text{SE}}^{\text{ind-cpa2-1}}(A) = 1] - \Pr[\text{Exp}_{\text{SE}}^{\text{ind-cpa2-0}}(A) = 1].$$

State and prove a proposition that captures the notion that any scheme SE which is IND-CPA security is also IND-CPA2 secure (IND-CPA \Rightarrow IND-CPA2). Use Proposition 5.12 from the BR notes and similar examples from class as guides. Be sure to clearly state your proposition the adversaries' advantages, running times, and numbers of oracle queries. In the proof, make sure you clearly describe the adversary's algorithm and how you calculate its advantage. Feel free to include a sketch to help explain your proof, but there must be a written specification of the adversary's algorithm that is understandable without the picture. In other words, a picture doesn't constitute a proof.

Problem 2. [10 points] Give a formal security definition capturing the notion of a symmetric encryption that hides message parity against chosen plaintext attack. The parity of a message is just the XOR of all its bits, i.e. the parity of $m = m_1 m_2 \dots m_\ell$ is equal to $\bigoplus_{i=1}^{\ell} m_i$.

Is this definition of security stronger or weaker than PR-CPA? Briefly justify your answer by explaining how you would go about proving it, but you need not give a formal proof.

Problem 3. [15 points] Consider the following simple symmetric block encryption algorithm where key $K \in \{0, 1\}^{64}$ and block size $n = 32$:

$$\text{Enc}_K(m) \stackrel{\text{def}}{=} (m \oplus K_0) \boxplus K_1,$$

¹This is just an annoying technicality. Don't let it distract you.

where K_0, K_1 denote the leftmost and rightmost 32 bits of K , respectively, and \boxplus denotes addition modulo 2^{32} .

- a) Specify the corresponding decryption algorithm for a ciphertext c .
- b) Suppose the adversary has access to two sets of plaintext and their corresponding ciphertexts and wishes to determine K . Write the two equations relating each ciphertext to its corresponding plaintext and derive a single equation in terms of one unknown (e.g. K_0). Is it possible to actually solve for K_0 ?
- c) Can you think of an attack that uses more than just a single pair of messages and ciphertexts to recover the key K ? Describe your attack and clearly state the number of plaintext, ciphertext pairs it requires. How likely is your attack to succeed in recovering the entire key K ?

Problem 4. [15 points] Consider the following method to verify that Alice and Bob are both in possession of the same secret key. Alice randomly chooses a random string of the same length as the key, XORs the random string with the key, and sends the result to Bob in the clear over whatever communication channel they share. Bob XORs the string he receives from Alice with his key (which should be the same) and sends back to Alice the result. If Alice receives from Bob her original random string she concludes they share the same key, and neither party had to transmit their key.

- a) Is there a flaw in this scheme? Clearly describe what you think the security and non-security goals for the protocol are and what adversary attack capabilities make sense.
- b) Describe an alternate protocol to accomplish the same task that utilizes either pseudorandom permutations or functions. Clearly state your assumptions, whatever information they should exchange, and the probability of error if any. Briefly explain why your protocol satisfies the criteria you gave in part a).

Problem 5. [30 points] Let $F : \{0, 1\}^\ell \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ be a family of pseudorandom functions. For each of proposed functions below state whether or not it is a PRF. If it is a PRF give a short proof (by contradiction) that describes how to convert an adversary for F' into an adversary for F . You need not compute the advantages, but for the proof to be valid, there should be some significant advantage ($2^{-\ell}$ or $2^{-\ell/2}$ aren't considered significant). The picture describing how to construct one adversary from the other is sufficient. If it isn't give a specific counter example, i.e. describe some F that is PRF, but for which F' is not. In the following \boxplus denotes addition modulo 2^ℓ .

- a) $F_K^1(x) \stackrel{\text{def}}{=} F_K(x) \boxplus F_K(\bar{x})$
- b) $F_K^2(x) \stackrel{\text{def}}{=} F_K(x) \oplus F_x(x)$
- c) $F_K^3(x) \stackrel{\text{def}}{=} F_{K_1}(x)$, where $K_1 = F_K(x)$
- d) $F_K^4(x) \stackrel{\text{def}}{=} F_{K_0}(x) \oplus F_{K_1}(x)$, where $K_0 = F_K(0^\ell)$ and $K_1 = F_K(1^\ell)$
- e) $F_K^5(x) \stackrel{\text{def}}{=} F_{K_1}(x) \boxplus F_{K_2}(x)$, where $K_1 = F_K(x)$ and $K_2 = F_{\bar{K}}(x)$

Problem 6. [HW Extra credit: 10 points] Show that for all $K \in \{0, 1\}^{56}$ and all $x \in \{0, 1\}^{64}$

$$\text{DES}_K(x) = \overline{\text{DES}_{\bar{K}}(\bar{x})}.$$

This is called the *complementation property* of DES.