CSC 5440: Cryptography
The Chinese University of Hong Kong

Midterm Exam
due Monday 14 March

Please turn in your solutions on **Monday 14 March by 4pm** in Andrej's office (SHB 926).

You must work on the problems and write up the solutions individually. No collaboration is allowed. You are free to consult the lecture notes, homework solutions, and references listed on the course web page. However, you are not allowed to look for solutions in external sources, including textbooks, other lecture notes, and the internet.

Use asymptotic definitions of security, unless specified otherwise. In all the problems, assume that (asymptotically secure) pseudorandom generators exist, and all schemes are private key.

Problem 1

This problem concerns the Goldreich-Goldwasser-Micali construction of pseudorandom functions $F\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$:

$$GGM(x, y) = G_{x_n}(G_{x_{n-1}}(\cdots G_{x_1}(y)\cdots))$$

In class we showed that if G_0 and G_1 are the left n bits and the right n bits of a pseudorandom generators $G\colon \{0,1\}^n \to \{0,1\}^{2n}$, then the $F_K(x) = GGM(x, K)$ is a pseudorandom function family. Show that, in general, $H_K(y) = GGM(K, y)$ is not a pseudorandom function family: There exists a pseudorandom generator G for which $\{H_K\}$ is not a pseudorandom function family.

Problem 2

Let (Tag, Ver) be a deterministic MAC that is secure against chosen message attack for messages of length m, key length k, and tag length t. Consider the following MAC (Tag', Ver') for messages of length $2m$ with key length $2k$:

$$Tag'((K_1, K_2), (M_1, M_2)) = Tag(K_1, M_1) + Tag(K_2, M_2)$$

$$Ver'((K_1, K_2), (M_1, M_2), T) = \begin{cases} 1, & \text{if } T = Tag'((K_1, K_2), (M_1, M_2)) \\ 0, & \text{otherwise.} \end{cases}$$

Is (Tag', Ver') secure against chosen message attack?

Problem 3

Let (Enc, Dec) be an encryption scheme with key length k for message length m. Consider the following encryption scheme (Enc', Dec') with key length k for message length $2m$:

$$Enc'(K, (M_1, M_2)) = (Enc(K, M_1), Enc(K, M_2))$$
$$Dec'(K, (C_1, C_2)) = \begin{cases} (Dec(K, C_1), Dec(K, C_2)), & \text{if } Dec(K, C_1), Dec(K, C_2) \neq \texttt{error} \\ \texttt{error}, & \text{otherwise.} \end{cases}$$

In case Enc is randomized, assume that the two calls to Enc are applied with independent randomness.

(a) Show that if (Enc, Dec) is CPA-secure, then (Enc', Dec') is CPA-secure.

(b) Show that (Enc', Dec') is not CCA-secure.

Problem 4

Alice and Bob are using an encryption scheme (Enc, Dec) with key length k for messages of length m. Suppose Eve has compromised the security of (Enc, Dec) as follows: Eve has found some small subset of messages $B \subseteq \{0,1\}^m$ so that Eve can now decrypt any ciphertext of the form $Enc(K, M)$ when M is in B (but finds no information about M from $Enc(K, M)$ if M is not in B).

To thwart this attack, Alice and Bob replace (patch) their encryption scheme (Enc, Dec) with a new scheme (Enc', Dec'). Say that (Enc', Dec') is a *secure patch* of (Enc, Dec) when the following is true: Even if Eve has the ability to obtain decryptions of ciphertexts $Enc(K, M)$ when $M \in B$ for some subset B of size $\varepsilon \cdot 2^m$, (Enc', Dec') is still secure.

(a) Give a formal definition of (s, ε) message indistinguishability for a secure patch under a chosen plaintext attack. The parameter ε plays two roles here: It bounds both the size of B and the success probability of the distinguisher.

Your definition should start like this: "Encryption scheme (Enc', Dec') is a CPA-secure patch of encryption scheme (Enc, Dec) if ..."

(b) Consider the following patch of encryption scheme (Enc, Dec):

$$Enc'(K, M) = (Enc(K, R), Enc(K, M + R)), \text{where } R \sim \{0,1\}^m \text{ is random}$$
$$Dec'(K, (C, C')) = Dec(K, C) + Dec(K, C').$$

Show that if (Enc, Dec) is (s, ε) CPA-secure, then (Enc', Dec') is an $(\Omega(s), O(\varepsilon))$ CPA-secure patch of (Enc, Dec).

(c) (Optional) If (Enc, Dec) is CCA-secure, is (Enc', Dec') a CCA-secure patch of (Enc, Dec)?