دانشکده ریاضی و آمار

مقدمه‌ای بر رمزنگاری زمان‌بارگذاری: ۳۰ اردیبهشت ۱۴۰۱

تمرین شماره ۲

مدرّس: مجتبی رفیعی تحویل نهایی: ۱۱ خرداد ۱۴۰۱

- Upload your answers on **LMS** with the name: **StudentNumber.pdf**
- Upload a PDF file. Image and zip formats are not accepted.
- Similar answers will not be graded.
- NO answers will be accepted via e-mail.
- You can't upload files bigger than 10 Mb, so you'd better type.
- Deadline time is always at 23:55 and will not be extended.
- This problem sets include 100+5 points.
- For any question contact Mojtaba Rafiee via `ui.cs.crypto.rafiee@gmail.com`.

Problem 1

(20 Points) Let $G_1, G_2 : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ be two PRGs. Which of the following is a PRG. Provide a proof or a counter-example for your answers.

1. $G(k_1||k_2) = G_1(k_1) \oplus G_2(k_2)$ with $|k_1| = |k_2|$
2. $G(k) = G_1(0^{|k|})||G_2(k)$
3. $G(k) = G_1(k) \oplus G_2(k)$
4. $G(k) = G_1(G_2(k))$

Problem 2

(20 points) For a given PRG $G : S \rightarrow \{0,1\}^L$, and a given adversary $\mathcal{A}$, consider the following attack game:

- The adversary sends an index i, with $0 \leq i \leq L-1$, to the challenger.
- The challenger chooses a random s from S and computes $r = G(s)$ and sends $r[0], r[1], ..., r[i-1]$ to the adversary. ($r[i]$ is the i'th bit of r)
- The adversary outputs $g \in \{0,1\}$.

We say that $\mathcal{A}$ **wins** if $r[i] = g$, and we define $\mathcal{A}$'s **advantage** $adv^{Pre}_{\mathcal{A},G}$ to be:

$$|\Pr[\mathcal{A} \text{ wins}] - \frac{1}{2}|$$

We say that G is ***unpredictable*** if the value of $adv^{Pre}_{\mathcal{A},G}$ is negligible for all p.p.t adversaries $\mathcal{A}$.

Show that if G is secure, then it is unpredictable

Problem 3

(25 points) For many block cipher encryption modes such as CBC mode, messages need to be a multiple of the block size. Messages that are not a multiple of the block size can still be encrypted, but need to be padded to a multiple of the block size. The padding moreover needs to be reversible so that the receiver can recover the original (unpadded)

message when decrypting. For each of the following padding schemes, decide if the padding is reversible: that is, for any message, after padding to a multiple of the block length, it is possible to recover the message again. If the padding is reversible, explain how to recover the message and why recovery is guaranteed to work. If not, explain how it fails.

1. (5 Points) Null Padding: Append 0's to the message until it is a multiple of the block length

2. (5 Points) Bit Padding, version 1: Let N be the number of bits necessary to add to the message for it to become a multiple of the block length. If $N > 0$, append 10^{N-1} (that is, a 1 followed by $N - 1$ 0's) to the message. If $N = 0$ (the message is already a multiple of the block length), do nothing.

3. (5 Points) Bit Padding, version 2: This is the same as part 2, except that in the case $N = 0$, we append an entire block, set to 10^{B-1} , where B is the block length in bits.

4. (5 Points) PKCS7 Padding: Assume the message is an integer number of bytes, but not an integer number of blocks. Let N be the number of bytes necessary to pad to a multiple of the block length. If $N = 0$ (which means the message is already a multiple of the block length) let N be equal to the block length (in bytes). Now pad with N bytes, each byte set to the value N. For example, if $N = 3$, append 3 bytes to the message, each byte set to 00000011.

5. (5 Points) PKCS7 padding, except that if the message is already a multiple of the block length, do not add any padding.

Problem 4

(20 Points) Suppose that $\{F_S : \{0,1\}^k \rightarrow \{0,1\}^k | \ S \in \{0,1\}^k\}$ is a pseudo-random family of functions from k-bit input to k-bit output, indexed by k-bit key (”seed”). We would like to get a new pseudo-random function family in which each function maps k bits to 2k bits. Consider the following construction, and for each show whether it is good or bad (namely whether the specified family is pseudo-random or not).

1. $F^1_S(x) = F_S(0^k)||F_S(x)$

2. $F^2_S(x) = F_S(x)||F_S(\bar{x})$

3. $F^3_S(x) = F_{0^k}(x)||F_S(x)$

4. $F^4_S(x) = F^1_S(x)||F^2_S(x)$,where $S_1 = F_S(0^k)$ and $S_2 = F_S(1^k)$

Problem 5

(20 points) What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

1. (10 Points) Each round function outputs all 0's, regardless of the input.
2. (10 Points) Each round function is the identity function.