دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری تحویل اصلی: ۲۳ آبان ۱۳۹۹

تمرین شماره ۲

مدرّس: دکتر شهرام خزائی *تحویل نهایی: ۳۰ آبان ۱۳۹۹*

- Upload your answers on courseware 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 2 Mb, so you'd better type.
- Deadline time is always at 23:55 and will not be extended.
- You should submit your answers before soft deadline.
- You will lose 5 percent for each day delay if you submit within a week after soft deadline.
- You can not submit any time after hard deadline.
- This problem set includes 90 points.
- For any question contact Aysan Nishaburi via `aysannishaburi@gmail.com`.

Problem 1

Let us see why in CBC mode an unpredictable IV is necessary for CPA security.

(a) (10 Points) Suppose a defective implementation of CBC encrypts a sequence of packets by always using the last ciphertext block of packet number i as the IV for packet number $i+1$ (up until a few years ago all web browsers implemented CBC this way). Construct an efficient adversary that wins the CPA game against this implementation with advantage close to 1. Recall that in the CPA game the attacker submits packets (a.k.a messages) to the challenger one by one and receives the encryption of those packets. The attacker then submits the semantic security challenge which the challenger treats as the next packet in the packet stream.

(b) (10 Points) Suppose the block cipher (E, D) used for CBC encryption has a block size of n bits. Construct an attacker that wins the CPA game against CBC with a random IV (i.e. where the IV for each message is chosen independently at random) with advantage close to $1/2^n$.

Your answer for part (b) explains why CBC cannot be used with a block cipher that has a small block size (e.g. $n = 32$ bits). Note that there are many other problems with such a small block size, which is why AES has a block size of 128 bits.

Problem 2

(20 Points) Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator. Define the keyed function $F : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^{2n}$ as $F_k(x) = G(x) \oplus k$. Prove that F is not a pseudorandom function by describing and analyzing a concrete distinguisher D.

Problem 3

(20 Points) Prove that the following encryption scheme is CCA secure. Let $\{p_k\}$ be a collection of pseudorandom permutations mapping $\{0,1\}^{3n}$ to $\{0,1\}^{3n}$.

- To encrypt $x \in \{0,1\}^n$ with key k do the following: choose $r \leftarrow_R \{0,1\}^n$, and send $p_k(x\|r\|0^n)$ (were $\|$ denotes concatenation).
- To decrypt $y \in \{0,1\}^{3n}$, compute $x\|r\|w = p_k^{-1}(y)$. If $w \neq 0^n$ then output $\perp$. Otherwise, output x.

Problem 4

Let F be a secure PRF defined over $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$, where $\mathcal{K} = \mathcal{X} = \mathcal{Y} = \{0,1\}^n$.

(a) (10 Points) Show that $F_1((k_1, k_2), (x_1, x_2)) := F(k_1, x_1) \oplus F(k_2, x_2)$ is not a secure PRF. That is, show an adversary $\mathcal{A}_1$ on F_1 that has non-negligible advantage in distinguishing $F_1(k, .)$ from a random function in $\text{Funs}[\mathcal{X}^2, \mathcal{Y}]$ (which is the set of all functions from $\mathcal{X} \times \mathcal{X}$ to $\mathcal{Y}$).

(b) (10 Points) Show that $F_2(k, x) := F(k, x) \| F(k, F(k, x))$ is not a secure PRF.

(c) (10 Points) Prove that $F_3(k, x) := F(k, x) \oplus x$ is a secure PRF. Do so by proving the contrapositive: show that if an adversary $\mathcal{A}_3$ can distinguish $F_3(k, .)$ from a random function then there is adversary $\mathcal{B}$ (that is a wrapper around $\mathcal{A}_3$) that can distinguish F from a random function. This $\mathcal{B}$ will play the role of challenger to $\mathcal{A}_3$, and attack F.