Assignment 2

1. Prove the equivalence of Definition 3.8 and Definition 3.9.

2. Let $|G(s)| = \ell(|s|)$ for some ℓ. Consider the following experiment:

   The PRG indistinguishability experiment $\mathrm{PRG}_{\mathcal{A},\mathcal{G}}$(n):

   (a) A uniform bit $b \in \{0,1\}$ is chosen. If b=0 then choose a uniform $r \in \{0,1\}^{\ell(n)}$;if b=1 then choose a uniform $s \in \{0,1\}^n$ and set $r := G(s)$.

   (b) The adversary A is given r,and outputs a bit $b^{'}$.

   (c) The output of the experiment is defined to be 1 if $b^{'} = b$,and 0 otherwise. Provide a definition of a pseudorandom generator based on this experiment, and prove that your definition is equivalent to Definition 3.14. (That is, show that G satisfies your definition if and only fi it satisfies Definition 3.14.)

3. Consider the following keyed function F: For security parameter n, the key is an $n \times n$ boolean matrix A and an n-bit boolean vector b. Define $F_{A,b} : \{0,1\}^n \rightarrow \{0,1\}$ by def: $F_{A,b}(x) = Ax + b$,where all operations are done module 2. Show that F is not a pseudorandom function.

4. Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$.For each of the following encryption schemes. State whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.)Explain your answer.

   (a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

   (b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$

   (c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$,then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$

5. Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

6. Assume secure MACs exist. Prove that there exists a MAC that is secure (by Definition 4.2) but is not strongly secure (by Definition 4.3).

7. Consider the following MAC for messages of length $\ell(n) = 2n - 2$ using a pseudorandom function F: On input a message $m_0 \| m_1$ (with $|m_0| = |m_1| = n - 1$) and key $k \in \{0,1\}^n$, algorithm Mac outputs $t = F_k(0\|m_0)\|F_k(1\|m_1)$. Algorithm Vrfy is defined in the natural way. Is (Gen, Mac, Vrfy) secure? Prove your answer.

8. Let F be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (in each case Gen outputs a uniform $k \in \{0,1\}^n$. let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)

   (a) To authenticate a message $m = m_1, \cdots, m_\ell$, where $m_i \in \{0,1\}^n$, compute $t := F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$.

   (b) To authenticate a message $m = m_1, \cdots, m_\ell$, where $m_i \in \{0,1\}^{n/2}$, compute $t := F_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle \| m_\ell)$.

   (c) To authenticate a message $m = m_1, \cdots, m_l$, where $m_i \in \{0,1\}^{n/2}$, choose uniform $r \leftarrow \{0,1\}^n$, compute

$$t := F_k(r) \oplus F_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle \| m_\ell),$$

   and let the tag be $\langle r, t \rangle$.

9. Prove that the following modification of basic CBC-MAC do not yield a secure MAC (even for fixed-length messages):

   (a) Mac outputs all blocks $t_1, \cdots, t_\ell$, rather than just t_ℓ. (Verification only checks whether t_ℓ is correct.)

   (b) A random initial block is used each time a message is authenticated. That is, choose uniform $t_0 \in \{0,1\}^n$, run basic CBC-MAC over the "message" $t_0, m_1, \cdots, m_\ell$, and output the tag $\langle t_0, t_\ell \rangle$. Verification is done in the natural way.

Note:

Definition 3.8: A private-key encryption scheme $\prod = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ has indistinguishable encryptions in the presence of an eavesdropper, or is EAV-secure, if for all probabilistic polynomial-time adversaries A there is a negligible function negl such that, for all n,

$$\Pr[PrivK_{A,\pi}^{eav} = 1] \leqslant 1/2 + negl(n).$$

Where the probability is taken over the randomness used by A and the randomness used in the experiment (for choosing the key and the bit b, as well as any randomness used by Enc).

Definition 3.9: A private-key encryption scheme has indistinguishable encryption in the presence of an eavesdropper if for all PPT adversaries A there is a negligible function negl such that

$$|Pr[out_A(PrivK_{\mathcal{A},\prod}^{eav}(n,0) = 1)] - Pr[out_A(PrivK_{\mathcal{A},\prod}^{eav}(n,1) = 1)]| \leqslant negl(n).$$

Definition 3.14: let ℓ be a polynomial and let G be a deterministic polynomial-time algorithm such that for any n and any input $s \in \{0,1\}^n$,the result G(s) is a string of length $\ell(n)$. We say that G is a pseudorandom generator if the following conditions hold: 1.(Expansion:) For every n it holds that $\ell(n) > n$. 2.(Pseudorandomness:)For any PPT algorithm D, there is a negligible function negl such that

$$|Pr[D(G(s)) = 1] - Pr[D(r) = 1]| \leqslant negl(n).$$

Where the first probability is taken over uniform choice of $s \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $r \in \{0,1\}^{\ell(n)}$ and the randomness of D.We call ℓ the expansion Factor of G.

Definition 4.2: A message authentication code $\prod = (\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$ is existentially unforgeable under an adaptive chosen-message attack, or just secure ,if for all probabilistic polynomial-time adversaries A, there is a negligible function negl such that:

$$\Pr[\mathrm{Mac} - \mathrm{forge}_{\mathcal{A},\prod}(n) = 1] \leqslant negl(n).$$

Definition 4.3: A message authentication code $\prod = (\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$ is strongly secure, or a strong MAC, if for all probabilistic polynomial-time adversaries $\mathcal{A}$, there is a negligible function negl such that:

$$\Pr[\mathrm{Mac} - \mathrm{sforge}_{\mathcal{A},\prod}(n) = 1] \leqslant negl(n).$$

(1) Due date: Sunday, October. 28, 2018, at 23:59. Send your assignment to both of the following emails: 2821785913@qq.com

(2) Assignment should be named by UNo+Name+A2.docx/doc/pdf.

(3) Penalty for late submission: 15% of the total marks for every day after the deadline.

(4) Answer ALL 10 questions.