密码学第一次作业

1.

(a)

1. **shift:**
   Gen: chooses a uniform k depend on security parameter
   Enc: $c_i = (m_i + k)\ mod\ 256$
   Dec: $m_i = (c_i - k)\ mod\ 256$
2. **Vigenere ciphers**
   Gen: Choose a random period: this can be chosen uniformly in a fixed set of some size, or it can be chosen according to some valid probability distribution over the integers (e.g., assign the length $5 + i$ with probability 2^{-i}). Denote the chosen period by t. For $i = 0, ..., t-1$ choose uniform k_i in $\{1, ..., 255\}$. Output the key $k = k_0, ...k_{t-1}$
   Enc: Given a plaintext $p = p_0, ..., p_n$ and a key $k = k_0, ..., k_{t-1}$,set $c_i := [p_i + k_{i\ mod\ t}]\ mod\ 256]$. Output $c_0, ...c_n$.
   Dec: Given a ciphertext $c_0, ...c_n$ and a key , set $p_i := [c_i - k_{i\ mod\ t}]\ mod\ 256]$. Output $p = p_0, ..., p_n$

(b)

1. **shift:**
   Ask for the encryption of any plaintext character p and let c be the ciphertext character returned; the key is simply $k := [c - p\ mod\ 256]$.
2. **Vigenere ciphers**
   If the period t is known then the encryption of a plaintext of length t (consecutive) suffices to recover the entire key.

2.

Encryption scheme Π is perfectly secret,so Π is indistinguishable.
Thus, we have $Pr[M = m|C = c] = Pr[M = m]$ and $Pr[M = m'|C = c] = Pr[M = m']$

every message $m, m' \in M$,we can get $Pr[M = m] = Pr[M = m']$

So $Pr[M = m|C = c] = Pr[M = m'|C = c]$

3.

(a)

Perfect security equals $Pr[Enc_K(M = m) = c] = Pr[Enc_K(M = m') = c]$

If the message is 0, then the ciphertext is 0 if and only if $k \in 0, 5$. So $Pr[Enc_K(0) = 0] = 1/3$. If the message is 1, then the ciphertext is 0 if and only if $k = 4$. So $Pr[Enc_K(1) = 0] = 1/6 \neq Pr[Enc_K(0) = 0]$

(b)

Prove that this is perfectly secret by analogy with the one-time pad.

4.

(a) Define A as follows: A outputs $m_0 = aab$ and $m_1 = abb$. When given a ciphertext c, it outputs 0 if the first character of c is the same as the second character of c, and outputs 1 otherwise. Compute $Pr[PrivK^{eav}_{A,\Pi} = 1]$.

(b) Construct and analyze an adversary A' for which $Pr[PrivK^{eav}_{A',\Pi} = 1]$ is greater than your answer from part (a).

5

If $s = 0^n$,then $G(s) = 0^{2n}$, while $TRG(s) = \{0, 1\}^{2n}$, for the attacker, it is no indistinguishable . so it is no a pseudorandom genenerator.

6

(a) F' is a pseudorandom function. A formal proof is omitted, butrelies on the observation that distinct queries to F'_k result in distinct
queries to F_k

(b) F' is not a pseudorandom function. To see this, consider queryingon the two inputs 0^{n-1} and $0^{n-2}1$. We have

$$F'_k(0^{n-1}) = F_k(0^n)||F_k(0^{n-1}1)$$

and

$$F'_k(0^{n-2}1) = F_k(0^{n-1}1)||F_k(0^{n-2}1^2)$$

note that the second half of $F'_k(0^{n-1})$ is equal to the first half of $F'_k(0^{n-2}1)$.

Formally, define the following attacker A given 1^n and access to some function g:

$A^g(1^n)$:

- Query $y_0 = g(0^{n-1})$ and $y_1 = g(0^{n-2}1)$
- Output 1 if and only if the second half of y_0 is equal to the first half of y_1

As shown above, we have $Pr_{k\leftarrow\{0,1\}^n}[A^{F'_k(\cdot)}(1^n) = 1] = 1$. But when g is a random function then y_0 and y_1 are independent, uniform strings of length $2n$, and so the probability that the secondhalf of y_0 is equal to the first half of y_1 is exactly 2^{-n}. Thus, $Pr_{f\leftarrow Func}[A^{f(\cdot)}(1^n) = 1] = 2^{-n}$, and the difference

$$|Pr_{k\leftarrow\{0,1\}^n}[A^{F'_k(\cdot)}(1^n) = 1] - Pr_{f\leftarrow Func}[A^{f(\cdot)}(1^n) = 1]|$$

is not negligible.

7

(a) This scheme does not even have indistinguishable encryptions in the presence of an eavesdropper because the ciphertext doesn't depend on the key. An eavesdropper can easily compute m from $c = \langle r, s\rangle$ by computing $m := G(r) \oplus s$.

(b) This scheme has indistinguishable encryptions in the presence of an eavesdropper. To see this, note that $F_k(0^n)$ is pseudorandom and so a proof of this fact follows from the proof of Theorem 3.18. The scheme is not CPA-secure because encryption is deterministic

(c) This scheme is CPA-secure. A proof of this is very similar to the proof of Theorem 3.31 except that Repeat denotes the event that $r-1$,r or $r+1$ is chosen in another ciphertext.