密码学期中考试

姓名__________ 学号 __________ 得分 __________

1.(20 points) Consider a Caesar shift cipher on the Roman alphabet of 26 characters. We map the letter to one of the numbers 0-25, say x and add a key value $k \in [0, 25]$ compute $y = x + k \mod 26$ and then map back to the alphabet. If k is chosen uniformly at random then this is perfectly secure.

(a) Show that if we expand the range of k to $[0, 30]$, the cipher is no longer perfectly secure.

(b) Typically, to achieve the uniformity required for perfect security, the key space needs to be a multiple of a size of the ciphertext space and the keys selected uniformly at random. However one can achieve perfect security by other means (e.g. using a non-linear KEYGEN algorithm). Can you design a KEYGEN algorithm on $[0, 30]$ to make the cipher perfectly secure?

2.(20 points) For each of the functions below, determine whether they are **necessarily** negligible functions of n and provide brief explanations for (d) and (e).

(a) $f_1(n) = 2^{-\sqrt{\log n}}$.

(b) $f_2(n) = n^{-\log\log\log n}$.

(c) $f_3(n) = \frac{n!}{n^n}$.

(d) $f_4(n) = (g(n))^n$, where $g(n)$ is a non-negligible function and $0 < g(n) < 1$ for all $n >= 1$.

(e) $f_5(n) = g(h(n))$, where both $g(n)$ and $h(n)$ are negligible (and positive).

3.(20 points) Consider a pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{2n}$, now define $G' = G(x)_{[0,n)}||G(G(x)_{[n,2n)})$, prove G' is a PRG or give a counter example.

4.(20 points) Assume Π is a CPA secure scheme with the key space $\{0,1\}^n$. Let Π' be a derived scheme such that the encryption of a message M is as follows:

$$Enc_K^{\Pi'}(M) = Enc_K^{\Pi}(M)||LSB(K)$$

where $LSB(K)$ is the least significant bit of K that is chosen uniformaly at random from the key space. Is Π' a CPA secure scheme or not? Prove your answer.

5.(20 points) In this problem, we study a MAC scheme based on the CFB encryption mode. We consider a block cipher

$$E : \{0,1\}^{64} \times \{0,1\}^{64} \to \{0,1\}^{64},$$

where $E_k(x) = E(k,x)$ denotes the encryption of the plaintext x under the key k. The CFB-MAC of a given message $m \in \{0,1\}^*$ with the key k is obtained by first encrypting m with E_k using the CFB encryption mode and then combining the output blocks by XORing them together.

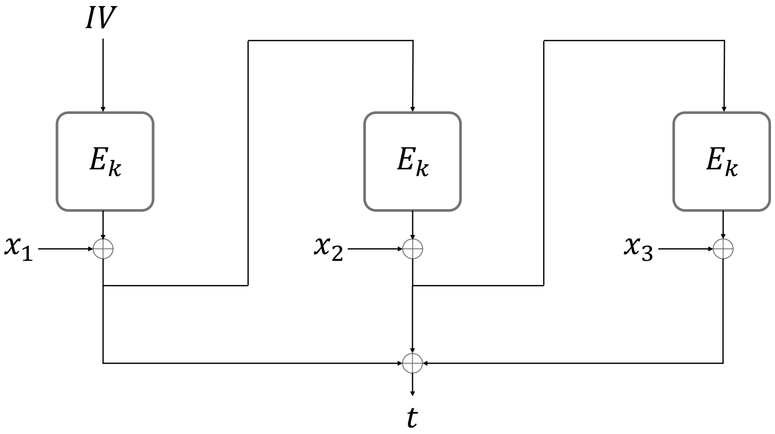
More precisely, for a message

$$m = x_1||x_2||\ldots||x_n,$$

we have

$$\text{CFB-MAC}_k(m) = y_1 \oplus y_2 \oplus \ldots \oplus y_n,$$

where $y_i = E_k(y_{i-1}) \oplus x_i$ for $i = 2,\ldots,n$ and $y_1 = E_k(IV) \oplus x_1$, IV being an initialization vector. For the sake of simplicity, we assume that all messages have a length that is a multiple of 64 bits. We also assume in all the questions of this problem that IV is constant and known.



(a) Assume we have access to an oracle $\mathcal{O}$ that computes the CFB-MAC under a given secret key k and a fixed known IV. Show that you can recover $E_k(IV)$ by querying only one message to the oracle.

(b) Assume we are given IV, $E_k(IV)$, and a $h \in \{0,l\}^{64}$. Show how it is possible to generate a message m of two blocks, such that $\text{CFB-MAC}_k(m) = h$.