CSE5014: Cryptography and Network Security
2023 Spring Semester Written Assignment # 2
Due: Apr. 11th, 2023, please submit at the beginning of class

Q.1 Let $negl_1$ and $negl_2$ both be negligible functions. Then prove that

(1) The function $negl_3$ defined by $negl_3 = negl_1(n) + negl_2(n)$ is negligible;

(2) For any positive polynomial p, the function $negl_4$ defined by $negl_4(n) = p(n) \cdot negl_1(n)$ is negligible.

Q.2 Prove that the property of computational indistinguishability: if $X_n \approx Y_n$ and f is a polynomial time computable function, then $f(X_n) \approx f(Y_n)$.

Q.3 Prove that if (Gen, Enc, Dec) is a *computationally secure* encryption with $\ell(n)$-long messages, then for every polynomial-time algorithm *Eve* and large enough n, the probability that Eve wins in the following game is smaller than 0.34:

1. Eve gets as inputs 1^n, and gives Alice three strings $x_0, x_1, x_2 \in \{0,1\}^{\ell(n)}$.
2. Alice chooses a random key $k \leftarrow_R \{0,1\}^n$ and $i \leftarrow_R \{0,1,2\}$ and computes $y = E_k(x_i)$.
3. Eve gets y as input, and outputs an index $j \in \{0,1,2\}$.
4. Eve *wins* if $j = i$.

Note: This proof can be generalized to show that the probability that Eve guesses which one of c messages was encrypted is at most $1/c + \epsilon(n)$ where ϵ is a negligible function.

Q.4 We call a sequence $\{X_n\}_{n\in\mathbb{N}}$ of distributions *pseudorandom* if it's computationally indistinguishable from the sequence $\{U_n\}$ where U_n is the uniform distribution over $\{0,1\}^n$. Are the following sequences pseudorandom? Prove or refute it.

1. $\{X_n\}$ where X_n is the following distribution: we pick $x_1, \ldots, x_{n-1}$ uniformly at random in $\{0,1\}^{n-1}$, and let x_n be the parity (i.e., XOR) of $x_1, \ldots, x_{n-1}$, we output $x_1, \ldots, x_n$.

2. $\{Z_n\}$ where for n large enough, with probability $2^{-n/10}$ we output an n bit string encoding the text "This is not a pseudorandom distribution" (say encode in ASCII and pad with zeros), and with probability $1 - 2^{-n/10}$ pick a random string. For n that is not large enough to encode the text, Z_n always outputs the all zeros string.

Q.5 Let G be a pseudorandom generator where $|G(s)| > 2|s|$. Take $s = s_1 \cdots s_n$, and for simplicity, n even.

(1) Define $G'(s) := G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?

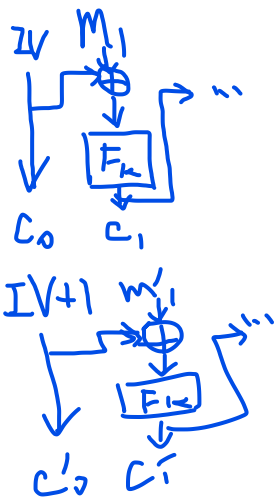
(2) Define $G'(s) := G(s_1 \cdots s_{n/2})$, where $s = s_1 \cdots s_n$. Is G' necessarily a pseudorandom generator?

Q.6 Define the keyed, length-preserving function F_k by $F_k(x) = F(k, x) = k \oplus x$. It is known that for any input x, the value of $F_k(x)$ is uniformly distributed if k is uniformly chosen. Prove or disprove that F_k is a PRF or not.

Q.7 Prove that if F_k is a length-preserving PRF, then

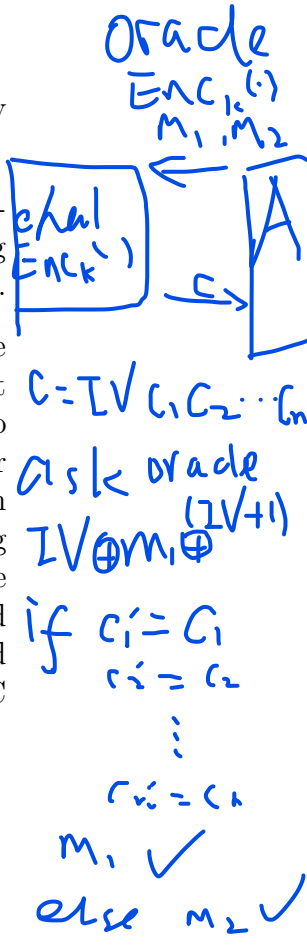
$$G(S) = F_s(\langle 1 \rangle)|F_s(\langle 2 \rangle)|\cdots|F_s(\langle \ell \rangle)$$

is a PRG with expansion factor $\ell \cdot n$, where $\langle i \rangle$ denotes the n-bit binary expression of the number i.



Q.8 Consider a 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.

Q.9 Recall that in the CBC mode (see Fig. Q.9 (1)), the ciphertext blocks are generated by applying the block cipher to the XOR of the current plaintext block and the previous ciphertext block, i.e., $c_0 = IV$ and then for $i = 1$ to ℓ, $c_i = F_k(c_{i-1} \oplus m_i)$; the final ciphertext is $\langle c_0, c_1, \ldots, c_\ell \rangle$. Now we consider a variant of the CBC mode, called *chained CBC* mode (see Fig. Q.9 (2)), in which the last block of the previous ciphertext is used as IV when encrypting the next message. This reduced the bandwidth, since the IV need not be sent each time. In Fig. Q.9 (2), an initial message m_1, m_2, m_3 is encrypted using a random IV, and subsequently a second message m_4, m_5 is encrypted using c_3 as the IV. However, the chained CBC mode is not as secure as CBC mode. Please provide a chosen-plaintext attack.



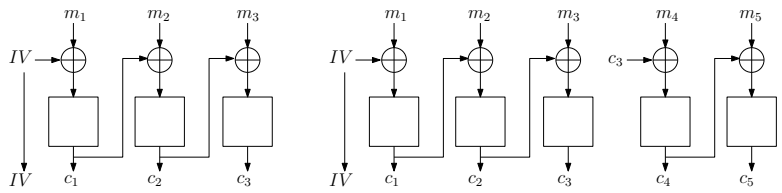


Figure 1: Q.9: CBC mode and Chained CBC mode