MATH 233: ASSIGNMENT 6

DUE: **FRIDAY, MARCH 29**, 11:59PM ON GRADESCOPE
UNIVERSITY OF ROCHESTER, SPRING 2024

Problem 1 (6.6.18)**.** Consider the following simplified version of the Cipher FeedBack (CFB) mode. The plaintext is broken into 32-bit pieces: $P = [P_1, P_2, \ldots]$, where each P_j has 32 bits, rather than the eight bits used in CFB. Encryption proceeds as follows. An initial 64-bit X_1 is chosen. Then for $j = 1, 2, 3, \ldots$, the following is performed:

$$C_j = P_j \oplus L_{32}(E_K(X_j)), \quad X_{j+1} = R_{32}(X_j) \parallel C_j,$$

where $L_{32}(X)$ denotes the leftmost 32 bits of X, $R_{32}(X)$ denotes the rightmost 32 bits of X, and $X \parallel Y$ denotes the string obtained by writing X followed by Y.

Then the ciphertext consists of 32-bit blocks $C_1, C_2, C_3, C_4, \ldots$. Suppose that a transmission error causes C_1 to be received as $\tilde{C}_1 \neq C_1$, but that $C_2, C_3, C_4, \ldots$ are received correctly. This corrupted ciphertext is then decrypted to yield plaintext blocks $\tilde{P}_1, \tilde{P}_2, \ldots$. Explain the decryption process, and show that $\tilde{P}_1 \neq P_1$, but that $\tilde{P}_i = P_i$ for all $i \geq 4$. This implies that one error only affects at most three blocks of the decryption. (*Hint.* The decryption is $P_j = C_j \oplus L_{32}(E_K(X_j))$.)

Problem 2. (a) Let

$$f(x) = x^5 + x^3 + 1 \quad \text{and} \quad g(x) = x^3 + x + 1$$

be two polynomials in $\mathbb{Z}_2[x]$. Find $\gcd(f(x), g(x))$ and two polynomials $h(x), k(x)$ in $\mathbb{Z}_2[x]$ satisfying

$$h(x)f(x) + k(x)g(x) = \gcd(f(x), g(x))$$

in $\mathbb{Z}_2[x]$. Use the result to find the multiplicative inverse of $g(x)$ in

$$GF(2^5) = \{p(x) \in \mathbb{Z}_2[x] : \deg p < 5\}$$

defined by $f(x)$.

(b) Consider $f(x)$ and $g(x)$ in part (a) as polynomials in $\mathbb{Z}_3[x]$ and answer the same questions. That is, find $\gcd(f(x), g(x))$ and two polynomials $h(x), k(x)$ in $\mathbb{Z}_3[x]$ satisfying

$$h(x)f(x) + k(x)g(x) = \gcd(f(x), g(x))$$

in $\mathbb{Z}_3[x]$. Use the result to show that $f(x)$ does not define a finite field with 3^5 elements.

Problem 3 (3.13.47, modified)**.** (a) Using the fact that the only irreducible polynomials in $\mathbb{Z}_2[x]$ of degree 1 or 2 are x, $x+1$, and x^2+x+1, show that x^4+x+1 is irreducible in $\mathbb{Z}_2[x]$. (*Hint.* Use part (a). If it factors, it must have at least one factor of degree at most 2.)

(b) Show that $x^4 \equiv x+1$, $x^8 \equiv x^2+1$, and $x^{16} \equiv x \pmod{x^4+x+1}$ in $\mathbb{Z}_2[x]$.

(c) Show that $x^{15} \equiv 1 \pmod{x^4+x+1}$ from Part (c). (*Hint.* We can divide each side of $x^{16} \equiv x$ by x. Why are we able to do so?)

Problem 4. Consider the simplified DES encryption method described in the lecture (see Slide 12).

(a) Use the expander function and S-Boxes given on Slide 13 and the keys given on Slide 14, verify the second and third rounds of encryption given on Slide 15.

(b) Verify the first round of the decryption on the slide 16. That is, execute the Feistel system beginning with $L_3 = 100001$, $R_3 = 011101$, and K_3, and verify that it yields outputs (R_2, L_2).

Problem 5 (7.7.2)**.** Bud gets a budget 2-round Feistel system. (Two rounds are identical, unlike the DES where the last round is slightly different from the previous rounds.) It uses a 32-bit L, a 32-bit R, and a 32-bit key K. The function is $f(R, K) = R \oplus K$, with the same key for each round. Moreover, to avoid transmission errors, he always uses a 32-bit message M and lets $L_0 = R_0 = M$. Eve does not know Bud's key, but she obtains the ciphertext for one of Bud's encryptions. Describe how Eve can obtain the plaintext M and the key K.

Problem 6 (7.7.5)**.** (a) Let $K = 111\ldots111$ be the 56-bit DES key (after discarding parity bits) consisting of all 1's. Show that if $E_K(P) = C$, then $E_K(C) = P$ where E_K is the encryption function using the key K, so encrypting twice with this key returns the plaintext. (*Hint.* The round keys are sampled from K. Decryption uses these keys in reverse order.)

(b) Find another key with the same property as K in part (a). (*Note.* Such key is called a **weak key**.)