Indian Institute of Technology Kharagpur

AUTUMN Semester, 2017-18
COMPUTER SCIENCE AND ENGINEERING
CS60065: Cryptography and Network Security
Mid–semester Examination

Full Marks: 50

Time allowed: 2 hours

INSTRUCTIONS: This exam is closed book and closed notes. Calculators are allowed.
ANSWER ALL QUESTIONS.

1. (a) Prove that for any odd integer p, $p^2 \equiv 1 \pmod 8$. (2 marks)
   (b) Suppose $a|c$ and $b|c$ with $gcd(a, b) = 1$. Prove that $ab|c$. (2 marks)
   (c) Suppose, the sequence of numbers $a_1, a_2, a_3, \ldots$ are generated such that $a_n \equiv p^{n+2} \pmod{24}$. Prove that if p is prime, then $a_{n+2} = a_n$, i.e. the sequence consists of cycles of length-2. (Hint: you might want to use the results you proved in parts (a) and (b).) (4 marks)
   (d) The *Least Common Multiple* (lcm) of two positive integers a and b is another positive integer m such that: (i) $a|m$ and $b|m$, and (ii) if $a|c$ and $b|c$ for some $c > 0$, then $m \leq c$. Prove that $\text{gcd}(a, b)\text{lcm}(a, b) = ab$. (4 marks)

2. (a) Suppose the keystream obtained from a 5-stage LFSR is 110100100001010. Find the recurrence relation used to generate the keystream. Show all intermediate steps. (8 marks)
   (b) The decryption operation in the *Hill Cipher* taught in class requires the inversion of a matrix over $\mathbb{Z}_{26}$. Consider a general setting where the encryption and decryption operations are defined over $\mathbb{Z}_p$, where p is prime. Prove that that the number of 2×2 matrices invertible over $\mathbb{Z}_p$ is $(p^2 - 1)(p^2 - p)$. (Hint: for an 2×2 matrix to be invertible over a field, its two rows must be linearly independent.) (4 marks)

3. (a) State and prove *Shannon's Theorem of Perfect Secrecy* (both the directions). (7 marks)
   (b) Suppose a random variable X takes $m > 1$ values, and one of the values among them occurs with probability $(1 - \epsilon)$, with $\epsilon \in (0, 1)$. Suppose the function $\eta(p)$ is defined as: $\eta(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$ for $p \in (0, 1)$. Prove *Fano's Inequality*: $H(X) \leq \eta(\epsilon) + \epsilon \log_2(m - 1)$. (5 marks)

4. (a) Consider a sequence of plaintext blocks $x_1 x_2 \cdots x_n$ is encrypted by a block cipher operating in the CBC mode. Suppose a *collision* is observed, i.e., there exists a pair (i, j) with $i < j$ such that $y_i = y_j$. Show that information about the plaintext can be extracted. (4 marks)
   (b) It is known that DES satisfies the complementary property: $\overline{DES_k(x)} = DES_{\overline{k}}(\overline{x})$. How can an adversary use this property to decrease the time complexity of exhaustive key search for 2-key version of 3-DES? (4 marks)
   (c) Find the multiplicative inverse of $(x + x^2)$ in $\mathbb{F}_{2^3}$, modulo $m(x) = 1 + x + x^3$. (6 marks)