A – 10
B – 11
C – 12
D – 13

CS60065

E – 14
F – 15

Indian Institute of Technology Kharagpur

AUTUMN Semester, 2016-17

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. This question paper has two pages. ANSWER ALL QUESTIONS.

$ap + bq = d$

1. (a) Suppose a and b are given positive integers. Define the set $T = \{ax + by \,|\, x, y \text{ are integers}\}$. Then, prove that T is the set of all multiples of $d = \gcd(a, b)$. (2 marks)

   (b) If $\gcd(a, b) = 1$, prove that $\gcd(a, a + b) = 1$. (2 marks)

   (c) Using the result proved in parts (a) and (b) above, or otherwise, prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$. (3 marks)

   (d) Prove that $\mathbb{Z}_m$ is a field if and only if m is prime. (5 marks)

2. (a) Determine the inverse of the following matrix over $\mathbb{Z}_{26}$, if it exists: $\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 21 \\ 17 & 2 \end{pmatrix}$ (4 marks)

   (b) Decryption of the *Hill Cipher* requires a matrix inversion operation to be carried out over a specified integer ring. Prove that if p is prime, the number of 2×2 matrices that are invertible over $\mathbb{Z}_p$ is $(p^2 - 1)(p^2 - p)$. (Hint: recall that a matrix is invertible if its rows are linearly independent. Matrix rows $\mathbf{v}_1, \mathbf{v}_2, \cdots \mathbf{v}_n$ are linearly dependent, if there exist scalars $\lambda_1, \lambda_2, \cdots \lambda_n$, not all zero, such that $\sum_{i=1}^{n} \lambda_i \mathbf{v}_i = 0$.) (4 marks)

   (c) Using the result obtained in part-(b), prove that the number of invertible $d \times d$ matrices over $\mathbb{Z}_p$ is $\prod_{i=0}^{d-1} (p^d - p^i)$. (Hint: you may consider using *mathematical induction*.) (4 marks)

3. (a) Prove that the decryption in a Fiestel structure can be done by applying the encryption algorithm with the key schedule reversed. (5 marks)

   (b) Prove that $\{02\} \cdot \{0E\} \oplus \{03\} \cdot \{09\} \oplus \{0D\} \oplus \{0B\} = \{01\}$, where the notation has its usual significance (Hint: note that this result partially justifies the InvMixComumns step of AES). (10 marks)

$H(X) = \sum_{x} \Pr[x] \log_2\left(\frac{1}{\Pr[x]}\right)$

4. (a) Consider a cryptosystem in which $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ and $\mathcal{C} = \{1, 2, 3, 4\}$. Consider the following encryption matrix:

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

Suppose the keys are chosen equiprobably, and the plaintext probability distribution is: $\mathbf{Pr}[a] = \frac{1}{2}$, $\mathbf{Pr}[b] = \frac{1}{3}$ and $\mathbf{Pr}[c] = \frac{1}{6}$. calculate $H(\mathbf{P})$, $H(\mathbf{C})$, and $H(\mathbf{K}|\mathbf{C})$. (6 marks)

(b) Prove that in any cryptosystem, $H(\mathbf{K}|\mathbf{C}) \geq H(\mathbf{P}|\mathbf{C})$. (5 marks)
