Mid-West University

**Examinations Management Office**

Surkhet, Nepal

Final Examination 2080

Level: B.Ed. / VII Semester FM: 60

Time: 3 hrs PM: 30

Sub: Basic of Cryptography (MATH 472)

*Candidates are requested to give their answers in their own words as far as practicable.*

Attempt All the Questions.

**Group 'B'** $5 \times 6 = 30$

1. List and define security services discussing each of them.

2. Define linear congruence. Solve the education. $3x + 4 \equiv 6(mod 13)$

3. What is transposition ciphers? Use the additive cipher with key=15 to encrypt the message "hello"

**Or**

Suppose Alice again enciphers the message "Enemy attacks to night" this time using the combined approach. The encryption and decryption.

4. Define the order of a group. If G is a finite group of order 'n' and H$\subseteq G$ such that O(H) = m then m|n.

5. Distinguish between diffusion and confusion.

6. Find the result of 1191432 using format factorization method.

**Or**

Define co-primes with examples. There are infinitely many primes.

**Group C** 2×10=20

7. Describe RSA Algorithm. Given, p=3, q=11 & e=7. Find n, $\emptyset(n)$ & $d$.

8. State and prove Chinese remainder theorem.

**Or**

Define ring with are example. Generate the elements of the field $GF(2^3)$. Using the irreducible polynomial $f(x) = x^3 + x^2 + 1$.

**THE END**

Mid-West University

# Examinations Management Office

Surkhet, Nepal

Final Examination 2080

B.Ed. Level /VII Semester

Sub: Basic of Cryptography (MATH 472)

**Roll No. ................**

**Group "A"** **10×1=10**

Tick (✓) the Best Answer.

1. Which one of the followings is not active security?
   a. Modification  b Repudiation
   c. Snooping  d. Replaying

2. Which one of the following properties is true?
   a. If $a|b$ and b=0 then $|a| \leq |b|$
   b. If $a|b$ & $a|c$ then $a|bx + cy$ for some x,y∈ $\mathbb{Z}$
   c. a|b & b|c then $a \nmid c$
   d. If a|b & a|c then $a \nmid bc$

3. If G is a cyclic group, then G is...
   a. abelian  b. permutation
   c. trivial  d. monoid

4. A non-trivial ring $\langle R, +, \cdot \rangle$ is said to be a field if it satisfied the following axioms.
   a. R has identity
   b. R is commutative
   c. Every non-zero element $a \epsilon R$ has multiplicative inverse $a^{-1}$ in R
   d. All of the above

5. Encryption transformations are known as
   a. diffusion  b. confusion
   c. diffusion & Confusion  d. none of the mentioned

6. For n input bits the number of substitution patterns are,
   a. 2n  b. 2n.!
   c. $\frac{1}{2n!}$  d. 2n!

7. Which one of the followings number is quadratic residue of 11?
   a. 6  b. 7
   c. 8  d. 9

8. In cryptography the order of the letters in a message is rearranged by,
   a. transpositional ciphers
   b. substitution ciphers
   c. transtositional & substitution ciphers
   d. quadratic ciphers.

9. ELGamal encryption system is...
   a. symmetric key encryption algorithm
   b. asymmetric key encryption algorithm
   c. not an encryption algorithm
   d. black cipher method

10. An asymmetric-key cipher uses ...
    a. one key  b. two key
    c. three key  d. four key