TRƯỜNG ĐẠI HỌC MỞ TP.HCM **KIỂM TRA: AN TOÀN BẢO MẬT THÔNGTIN**

KHOA CÔNG NGHỆ THÔNG TIN Thời gian làm bài : 60’

Đề thi gồm 02 trang

ĐỀ 2

•**1.** Cho k = 45, N = 26, giải mã văn bản, dùng thuật mã Caesar:
với C = TGMHTGMAHGZMBG

•**2.** Cho k = BIMAT, N = 26, mã hóa văn bản, dùng thuật mã Vigenere :
với p= VANHOAXAHOI

•**3.** Cho k = BIMAT, N = 26, giải mã văn bản,dùng thuật mã Playfair:

C = KHHBMDOLMBOPTBLKHOEZDTFS

•**4.** Cho k = SVTK, N = 26, mã hóa văn bản,dùng thuật mã Playfair:

P = NANGDONGSANGTAO

•**5.** Cho bản rõ “CANNHANGOAIO” khóa k là:

9 7

3 4

Mã hóa bản mã với khóa k theo hệ mã Hill, tìm bản mã ? Biết hàm mã y=xk
•**6.** Cho bản mã “SGANLVEKBGAUKPDY” khóa k là:

9 7

3 4

Giải mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã y=kx

•**7.** Cho bản rõ "MUATHUHANOI" khóa k là:

8 3

5 3

Mã hóa với khóa k theo hệ mã Hill tìm bản mã ? Biết hàm mã y=kx

•**8.** Cho bản mã "EVDENNRP" khóa k là:

8 3

5 3

Giải mã với khóa k theo hệ mã Hill tìm bản rõ ? Biết hàm mã y=xk

•**9.** Người A chọn các thông số p =19, q = 7, e = 13. Hỏi khóa riêng của A là gì theo thuật mã RSA?

•**10.** Người A chọn các thông số p =33, q =17, e = 31. Hỏi cặp khóa công khai, riêng của A theo thuật mã RSA là gì ?

•**11.** Cho bản mã y = 18, khóa công khai n = 221, e = 71. Mã hóa với khóa trên theo hệ mã RSA tìm bản mã ?

•**12.** Người A chọn các thông số p =19, q =37, e = 137. Khi giải mã bản mã C = 196 theo thuật mã RSA ta sẽ thu được bản rõ nào sau đây ?

•**13.** Cho A,B chọn 2 số nguyên tố chung là g=2 , p = 23, a=17, b= 13. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman?

•**14.**Người A,B chọn 2 số nguyên tố chung là g=2 , p = 997, a=17, b= 19. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman ?

---------- oOo ----------