

## ĐỀ 1

•1. Cho  $k = 31$ ,  $N = 26$ , giải mã văn bản, dùng thuật mã Caesar:  
với  $C = \text{FSYTFSGFTRFY}$

•2. Cho  $k = \text{VAN}$ ,  $N = 26$ , mã hóa văn bản, dùng thuật mã Vigenere :  
với  $p = \text{VANHOANGHETHUAT}$

•3. Cho  $k = \text{BIMAT}$ ,  $N = 26$ , giải mã văn bản, dùng thuật mã Playfair:

$C = \text{KHHBMDOLMBOPTBATBAMY}$

•4. Cho  $k = \text{SVTK}$ ,  $N = 26$ , mã hóa văn bản, dùng thuật mã Playfair:

$P = \text{CHUYENCANCHAMCHI}$

•5. Cho bản rõ “THANHPHOMUABAY” khóa  $k$  là:

6      5

3      4

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

•6. Cho bản mã “THNANDIZMOAETQFO” khóa  $k$  là:

6      5

3      4

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

•7. Cho bản rõ “NOIVONGTAYLON” khóa k là:

7      2

3      3

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

•8. Cho bản mã “TEMSNCXX” khóa k là:

7      2

3      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  $p=19$ ,  $q=3$ ,  $e=5$ . Hỏi khóa riêng của A là gì theo thuật mã RSA?

•10. Người A chọn các thông số  $p=23$ ,  $q=17$ ,  $e=37$ . Hỏi cặp khóa công khai, riêng của A theo thuật mã RSA là gì ?

•11. Cho bản mã  $y=18$ , khóa công khai  $n=221$ ,  $e=91$ . Mã hóa với khóa trên theo hệ mã RSA tìm bản mã ?

•12. Người A chọn các thông số  $p=17$ ,  $q=37$ ,  $e=131$ . Khi giải mã bản mã  $C=240$  theo thuật mã RSA ta sẽ thu được bản rõ nào sau đây ?

•13. Cho A,B chọn 2 số nguyên tố chung là  $g=2$ ,  $p=29$ ,  $a=11$ ,  $b=13$ . 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  $g=2$ ,  $p=877$ ,  $a=23$ ,  $b=13$ . Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman ?

----- oOo -----