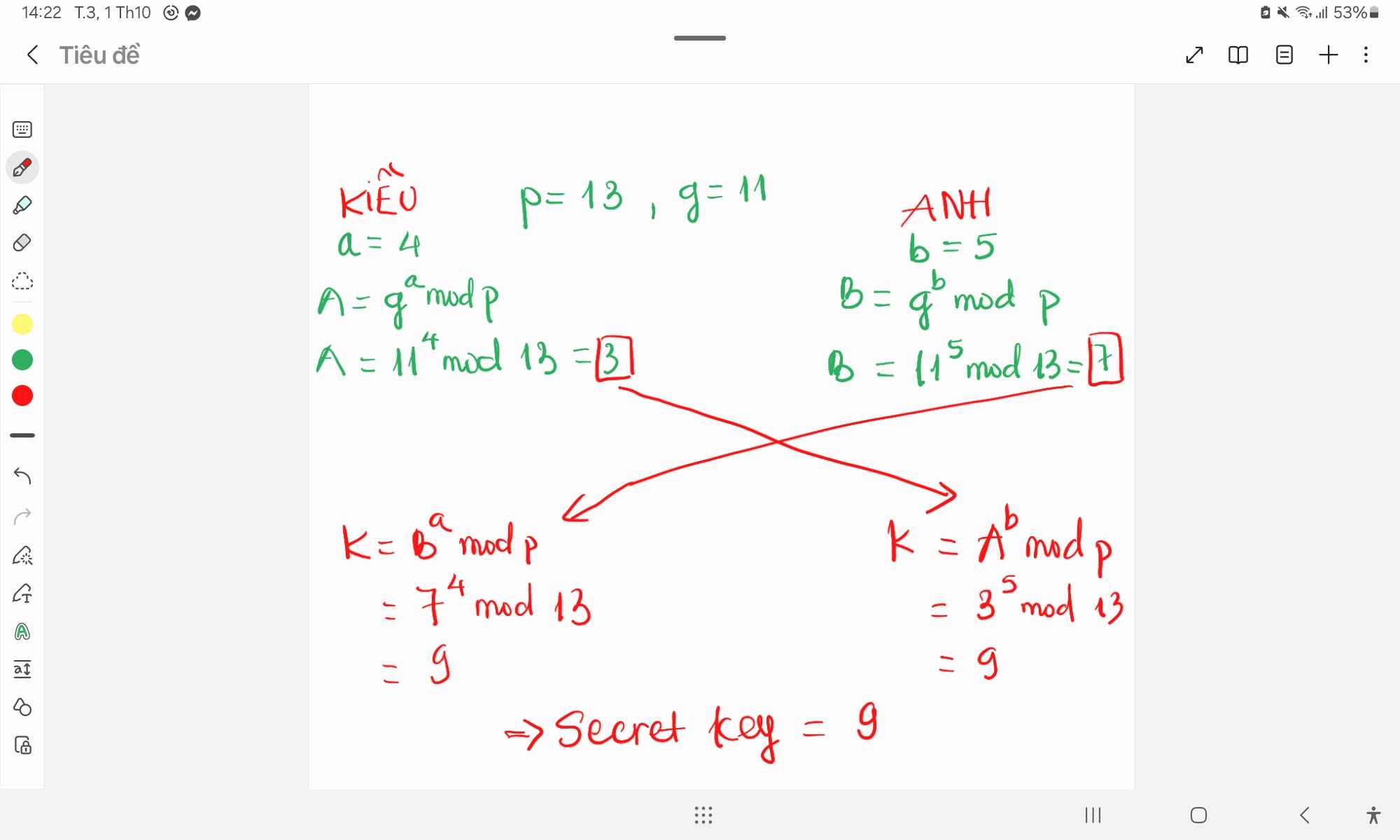
**Bài tập An toàn mạng máy tính**

**Lê Ngọc Kiều Anh - 22520047**

**Bài 1. Cho ví dụ về giải thuật trao đổi khóa Diffie Hellman**



**Bài 2. Mã hóa tên của mình bằng giải thuật RSA, biết p = 23, q =41, e = 13**

**Mã hóa tên: LENGOCKIEUANH**

Tên tương ứng với mã ASCII:

76 69 78 71 79 67 75 73 69 85 65 78 72

**n = p.q = 23.41 = 943**

**phi(n) = (p-1).(q-1) = 880**

**e = 13**

**d = 677**

**C = Me  mod n**

76 = 76^13 mod 943 = 181

69 = 69^13 mod 943 = 276

78 = 78^13 mod 943 = 633

71 = 71^13 mod 943 = 280

79 = 79^13 mod 943 = 659

67 = 67^13 mod 943 = 732

75 = 75^13 mod 943 = 726

73 = 73^13 mod 943 = 729

69 = 69^13 mod 943 = 276

85 = 85^13 mod 943 = 325

65 = 65^13 mod 943 = 306

78 = 78^13 mod 943 = 633

72 = 72^13 mod 943 =722

C = 181 276 633 280 659 732 726 729 276 325 306 633 722

**Bài 3.**

**- Với p = 5, q = 7, e = 5, các chữ cái (viết hoa) được đánh số từ 0 trở đi, giả sử nhận được thông điệp là 17 19 7 9 0 12 24. Hãy gải mã thông điệp này.**

**- Từ dữ liệu đã biết hãy thực hiện mã hóa thông điệp “BAO MAT THONG TIN”**

n = p.q = 35

phi(n) = (p-1).(q-1) = 24

e = 5

Giải mã: 17 19 7 9 0 12 24

C = Me  mod n

C1 = 17^5 mod 35 = 12

C2 = 19^5 mod 35 = 24

C3 = 7^5 mod 35 = 7

C4 = 9^5 mod 35 = 4

C5 = 0^5 mod 35 = 0

C6 = 12^5 mod 35 = 17

C7 = 24^5 mod 35 = 19

Thông điệp được giải mã: 12 24 7 4 0 17 19

Text: M Y H E A R T

Các chữ cái “BAO MAT THONG TIN” được chuyển thành dãy số tương ứng là: 1, 0, 14, 12, 0, 19, 19, 7, 14, 13, 6, 19, 8, 13

C = M5 mod 35

C1 = 1^5 mod 35 = 1

C2 = 0^5 mod 35 = 0

C3 = 14^5 mod 35 = 14

C4 = 12^5 mod 35 = 12

C5 = 0^5 mod 35 = 0

C6 = 19^5 mod 35 = 19

C7 = 19^5 mod 35 = 19

C8 = 7^5 mod 35 = 7

C9 = 14^5 mod 35 = 14

C10 = 13^5 mod 35 = 13

C11 = 6^5 mod 35 = 6

C12 = 19^5 mod 35 = 19

C13 = 8^5 mod 35 = 8

C14 = 13^5 mod 35 = 13