2.1

KNXMNSLKWJXMBFY JWGJSIXFIRNY XB

TWIKNXMWFSITAJWMJQRNSLFSDIFD

Dùng cryptotools phân tích thấy có chữ F I J N S W X có số lần xuất hiện nhiều nhất

và dựa vào bảng số lần xuât hiện của bảng chữ cái tiếng anh

ta có các chữ cái xuất hiện nhiều như A E H I N O T và lần lượt đoán xem key sẽ là bao nhiêu?

vd: A so với F key 5

E so với I key 5

H so với J key 2

H so với N key 6

I so với N key 5

N so với S key 5

như vậy ta có thể thấy key =5 xuất hiện nhiều nên suy ra đoạn ciphertext trên đã được mã hóa theo key = 5

và ta giải mã ngược lại như sau

plaintext:

FISHINGFRESHWAT ERBENDSADMIT SW

ORDFISHRANDOVERHELMINGANYDAY

4.1

a/ 3 keys

b/6 keys

c/28 keys

4.2

a/10 keys

b/20keys

c/classical: 1 key

public: 2 keys

4.3

a/1 key and 16 subkeys

b/5 key and 16 x 5 subkeys node mới tạo ra và 5 key and 16 x 5 subkeys các node cũ muốn giao tiếp với new node

c/1 node 5 public keys

6 nodes 30 plublic keys

4.4/

a/10 keys(include 5 private keys and 5 public keys)

b/6 public keys nó tạo ra tới các node còn lại và 6 public keys node tới node mới

c/6 nodes x 1 key x 6 nodes(khác) x 16 subkeys x 6 nodes(khác)

4.5/

a/Có node A ta có 10 key and 10 x 16 subkeys

không node A ta có 4 key and 4 x 16 subkey

b/

có node A ta có 8 public keys

Không có A ta có 4 public keys

4.6/

a/7 keys

b/14 keys