Exam 1 Sample

In answers to all questions, be as specific and formal as possible.
Neatness counts!

---

1. Multiple choice problems: choose the best answer for each problem.

1.1 Which of the following is not a symmetric cipher: _______

a) Playfair
b) DES
c) RSA
d) Caesar

symmetric cipher :
use the same key to
decode and encode

1.2 Which of the following could NOT be used to determine if a piece of ciphertext is likely the result of a simple substitution:________

a) Hashing
b) Letter frequency count
c) Digram count
d) Trigram count

kansj/I
yhwbc
def g l
mopqr
tuvxz

my so ft wa re
ne ve rh as bu
gs it ju st de
ve lo ps ra nd
om fe at ur es

td aq dv hn ol
af uf oc..

2. Playfair

Use playfair cipher to encrypt the following text. Note: treat I and J as the same character; use x as the dummy character.

`my software never has bugs it just develops random features`

The key is `kansasjayhawks`

3. RSA

3.1 In RSA, we pick p=5, q=11. Please continue to generate a set of public and private keys.

n =pq = 55
4*10 = 40
prime number 3
d =2*40+1 = 81/3
= 27

public <3,55>
private <27,55>

3.2 Please use your keys to encrypt message: "EECS". To convert characters to integer values, please encode a->1, b->2, c->3, etc.

5,5,3,19
c = me mod n = m^3 mod 221
m=cd modn=c^27 mod221

3.3 Is it hard to break the encrypted message in question 3.3? Why?

Easy! Attacker knows the public key. N is very small, it's easy to compute p and q from N.
Note: attackers do not know \phi(n). They have to compute \phi(n) from p and q.

3.4 Why is it hard to break an encryption done by (general) RSA?

In real world, p and q are very large prime numbers, hence, N is a very large number. It is computationally very expensive to factor N to get p and q.

Answers:

1.1: C: RSA. We all know that RSA is asymmetric
1.2: A

2.Playfair

```
td aq dv hn ol af uf oc nj hx qb kz az kx ef uf er qn oj kf
po gf ku zo ga
```

J could be I

3. RSA

3.3: Easy! Attacker knows the public key. N is very small, it's easy to compute p and q from N.
Note: attackers do not know \phi(n). They have to compute \phi(n) from p and q.

3.4 In real world, p and q are very large prime numbers, hence, N is a very large number. It is computationally very expensive to factor N to get p and q.