Cryptography Final - May 14th 2:45pm
Review Sheet

Need to know:

- Advantages and Disadvantages of one time pad
  - **Advantages:**
    - Impossible to crack if the key is never reused, completely random and kept secret
    - Immune to brute force attacks - trying all keys simply yields all plaintexts, all equally likely to be the acual plaintext.
  - **Disadvantages:**
    - Hard to find a truly random key, possible by: psuedorandom number generator
    - Security of the one time pad is only as secure as the exchange of the key - if this is not secure, then the key isn't either.
    - It is difficult to make sure that it continues to remain a secret - dispose of it after first use properly.
- Difference between Stream Ciphers and block ciphers
  - **Block Ciphers:**
    - More general i.e. can you convert a block cipher into a stream cipher? Yes, make block size one bit
    - Have no math involved - has to be reversable function
    - Are good in hardware and software but not as good in terms of hardware as stream cipher
  - **Stream Ciphers:**
    - stream ciphers have more mathematical structure - statistical attacks - easier to break and easier to study
    - stream ciphers are not suitable for software but highly efficient in hardware
  - What is 3DES - three 56 bit keys
    - Keys to test in worse case $2^{56\cdot 3}$, average 2^{55*3}
    - 3DES takes in 3 keys, and uses the first key to encrypt a message, the second key to decrypt the encrypted message and then uses the third key to reincrypt the decrypted message.
  - DES - bit length, keys to test in worse case
    - Keys to test in worse case 2^{56}, average 2^{55}
  - Why is 2 DES not secure?
    - Not secure because the brute force attack of it is less than 2^{90}.
    - Keys to test in worse case $2^{56\cdot 2}$.
    - 2DES takes 2 keys and encrypts the message with one of them and then decrypts with the other key.
  - What is meet in the middle attack - cuts in half the amount of keys to check
  - BC what is one time pad - attacks on one time pad - use same key - xoring two messages together gets the messages concatenated together.
- Brute force attacks and time it will take to do.

  - How to brute force decrypt something.

- Most likelyhood of something to happen probability
- Factorization of a number made of 2 primes - product of 3 primes instead of 2 primes
  - how to find phi with 3 prime values
  - given some cipher from Alice, how would you decrypt it?
  - think about it for every algorithm thats out there
  - also think about chinese remainder theorem
- diffie helman - given g^a and g^b, finding g^{ab} is hard... how?
  - given generator, compute the g^{ab}
  - Elgamal- how it works.
  - how to involve 3 people into this?
  - sending encrypted message from alice to bob, you have g^{ab} and for bob and carol you get g^{bc}.
  - m = 59, g = 2, p = 227. Alice has a = 8, bob b = 6, carol c = 5. $H_a = 29$, $H_b = 64$, $H_c = 32$ (all mod 227). Alice will generate g^{ab} using Bobs half mask. $F_{ab} = 12$. If you don't get the same full mask for bob and alice, its wrong. Same thing for bob and carol. $F_{bc} = 44$
  - p = 2q+1 - safe prime
  - q = $\frac{p-1}{2}$
  - $g^1 \neq 1$
  - $g^2 \neq 1$
  - $g^q \neq 1$
- Diffie helman - Elliptic Curve
  - Same security in EC - 128 as Elgamal 256.
  - Given a curve, only thing on the curve will be the quadratic residues.
  - given a set, show me a formula to find the quadratic residues. - Legranges symbol. $(\frac{x}{p}) = x^{\frac{p-1}{2}} mod\ p$ if we get 1, it is a quadratic residue, -1 is going to be a non quadratic

residue.

- finding the square roots of x raise x to the (p+1)/4 and mod by p

- get ascii character to the (x1, y1) character when turning it into a cipher - m is a point on the curve. ALICE has her own multiplier, bob will have his own multiplier. - use them to encrypt their own half masks B = 4g and A = 3g. F = B * 3 (bobs halfmask times Alice's multiplier.

- make sure you can find all of the points on the curve. you dont have to find the square roots if the number is not -1 when raised to the power of (p-1)/2 mod the number.
- the generator value is a point on the curve and the message point is a point on the curve. ALL OF THE THINGS YOU GET IS A POINT ON THE CURVE.

(1) RSA - Public Key Encryption.
Given:
n a small prime
e smallest odd integer with gcd with ϕ of 1
c an encrypted message
Needed:
p and q two prime numbers whose products are n
$\phi = (p-1)(q-1)$
$d = e^{-1}$

(a) Find the primes p and q. If you do not have a prime factorization on your calculator, then know that one of them is going to be less $\sqrt{n}$, knowing this, we can test all primes less than $\sqrt{n}$.

(b) Calculate $\phi = (p-1)(q-1)$. From here, it should be easy to find e if it is not given. Parse through lowest odd values until you find one where $gcd(e, \phi) = 1$.

(c) Now that you have e, you have to use pulverizer to solve for d.

ϕ	e	Quotient	Remainder	x_1	y_1	x_2	y_2