

# Cryptography Final - May 14th 2:45pm

## Review Sheet

### Need to know:

- Advantages and Disadvantages of one time pad
  - **Advantages:**
    - \*
- Difference between Stream Ciphers and block ciphers
  - block ciphers are more general - can you convert a block cipher into a stream cipher - yes, make block size one bit
  - stream ciphers have more mathematical structure - statistical attacks - easier to break and easier to study
  - block ciphers have no math involved - has to be reversible function
  - stream ciphers are not suitable for software but highly efficient in hardware
  - block ciphers are good in hardware and software but not as good in terms of hardware as stream cipher
  - BC what is one time pad - attacks on one time pad - use same key - XORing two messages together gets the messages concatenated together.
  - What is 3DES - bit length, keys to test in worst case  $2^{56}$ , average  $2^{55}$  - encryption decryption and encryption
  - DES - bit length, keys to test in worst case
  - Why is 2 DES not secure - how does it work
  - What is meet in the middle attack - cuts in half the amount of keys to check
- Brute force attacks and time it will take to do.
  - How to brute force decrypt something.
- Most likelihood 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 that's out there
- also think about Chinese remainder theorem
- Diffie-Hellman - 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 Bob's half mask.  $F_{ab} = 12$ . If you don't get the same full mask for Bob and Alice, it's 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-Hellman - 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. - Legendre's symbol.  $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \bmod p$  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  $(x_1, y_1)$  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  $A = 3g$ .  $F = B * 3$  (Bob's 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  $(p-1)/2 \bmod p$ .
- 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  $\gcd(e, \phi)$  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  $d$ .

| $\phi$ | $e$ | Quotient | Remainder | $x_1$ | $y_1$ | $x_2$ | $y_2$ |
|--------|-----|----------|-----------|-------|-------|-------|-------|
|--------|-----|----------|-----------|-------|-------|-------|-------|