Final

30 April 2014, 11:00–1:30 PM

There are six problems each worth five points for a total of 30 points. Show all your work, partial credit will be awarded. Space is provided on the test for your work; if you use a blue book for additional workspace, sign it and return it with the test. No notes, no collaboration.

Name: ____________________

Problem	Credit
1	
2	
3	
4	
5	
6	
Total	

1. *Diffie-Hellman:* In the integers mod 17, 5 is a generator. In the Diffie-Hellman protocol, Alice chooses 3 and Bob chooses 7.

   (a) What is the public number announced by Alice?

   (b) What is the public number announced by Bob?

   (c) What is the shared secret?

   Suppose instead of 5, the number 13 is used. What is the problem with using 13? Can you explain this in terms of the value $\phi(17)$, the size of $\mathbf{Z}_{17}^*$, the group of invertables mod 17.

2. *Adding points on an Elliptic Curve:* Consider the elliptic curve $y^2 = x^3 + 2x + 2 \bmod 17$. Let $P = (5, 1)$. Find $2P$, $4P$, $8P$ and then $11P$.

3. *El Gamal Signature weakness:* Let p be a prime, α a generator of $\mathbf{Z_p}$, and $\beta = \alpha^d \bmod p$ where d is secret.

   El Gamal Signatures on a message x is the pair of numbers:

   $$r = \alpha^{k_E} \bmod p, \quad s = (x - dr)k_E^{-1} \bmod p - 1,$$

   with verification equation:

   $$\alpha^x == \beta^r r^s \bmod p.$$

   The value k_E must be chosen randomly.

   (a) Show that signing two different messages x_1 and x_2 with the same value of k_E will reveal the secret d.

   (b) How will the attacker know that the value of k_E is the same for two signatures?

4. *Square root of -1:* A square root of -1 mod p would be an x such that $x^2 = -1$ mod p. For some primes such a square root exists, for others it does not.

   Use the formula for the quadratic residue (or any other method) to tell if there is a square root of -1 for the following primes, and if so, find a square root of -1 (show work):

   (a) 5

   (b) 7

   (c) 11

   (d) 13

   (e) 19

   Show that if there is a square root of s of -1 mod p, then the four numbers $s, -s, -1$ and 1 are all the fourth roots of 1.

   Give a simple condition on p for whether -1 has a square root mod p.

5. *Time space tradeoff:* Let $E_1(k, x)$ and $E_2(k, x)$ be two encryptions. In the notation, k is the key, and x is the plaintext.

   Consider the double encryption $E_2(k_2, E_1(k_1, x))$, where each k_1 and k_2 have b bits. We will try a known plaintext attack agains this double encryption.

   Let $y = E_2(k_2, E_1(k_1, x))$.

   (a) Suppose we use brute force to find the keys k_1, k_2 given x, y by trying all keys. What is the time for this attack?

   (b) Suppose we are given ample space, describe a much more efficient attack.

   (c) For the more efficient attack, how much space is needed?

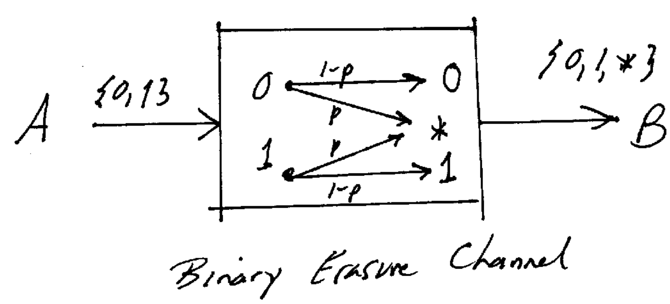
   (d) For the more efficient attack, how much time is required?

6. *An unbreakable protocol for bit commitment:*

Bit commitment is a protocol in which Alice commits to a bit by providing Bob with some data called the *commitment*. Later, Alice can open the commitment to substantiate which bit she had chosen.

- Bob cannot tell which bit Alice has has chosen only from the commitment.
- Alice can open the commitment in only one way: she cannot "cheat" having committed to a 1 to open her commits to convince Bob she had committed to a 0.

A *binary erasure channel* is a communication channel which transmits a 0 or a 1 between Alice and Bob. With probability p the bit provided by Alice is received by Bob as an "erasure", denoted $*$, and with probability $(1-p)$ it is received by Bob unchanged. Bob does not know if a $*$ received was the erasure of a 0 or 1. Alice does not know if Bob received her bit or the erasure $*$.



continued ...

An unbreakable protocol for bit commitment continued ...

Show how to do bit commitment using a binary erasure channel.

Hint: Have Alice choose a bunch of bits r_i to send to Bob via the erasure channel, as the commitment. (What constraint should there be on the r_i?) Later Alice will open the commitment by sending the r_i again this time by a perfect channel which does not erase the bits. (What should Bob check?)

Questions to answer:

- Why can't Alice successfully cheat? Why is it important Alice not know if a bit is erased?
- Why doesn't Bob know the choice from the commitment? Why is it important that Bob doesn't know the value of the bit erased?
- How is this protocol "unbreakable"?