SPCS CRYPTOGRAPHY
HOMEWORK SOLUTIONS

Homework 1

Reference for today's lecture: Chapter 1 - Chapter 4.2 of textbook.

1. Send me an email and tell me what you think about the class today, but **encrypt** your comment using one of the ciphers we discussed.

2. We can use the cipher wheel (Figure 1) to encrypt/decrypt messages. Here the outer wheel is the plaintext and the inner wheel is the ciphertext. For example, `a` is encrypted as `T`, `g` is encrypted as `Z`, and `fun` is encrypted as `YNG`.
   (a) Encrypt the following text,

   `the quick brown fox jumps over the lazy dog`

   Solution. MAX JNBVD UKHPG YHQ CNFIL HOXK MAX ETSR WHZ
   (b) Decrypt the following sentence,

   `Rxl mabl bl max vhkkxvm tglpxk`

   Solution. yes this is the correct answer
   (c) Decrypt the following sentence,

   `Mh ux hk ghm mh ux matm bl max jnxlmbhg`

   Solution. To be or not to be that is the question

FIGURE 1. Picture taken from a blog, *The Asylum*.

3. Sometimes when you run the Caesar cipher, one English word becomes another. For example, "$COLD$" becomes "$FROG$" if we shift everything to the right by 3. In this case we say that the **shift key** is 3.

   Figure out which word each of the following can be encrypted to. Pick any three parts for your problem set.

   (a) FOLK
   Solution. IRON, 3
   (b) DAZED
   Solution. SPOTS, 11
   (c) ALOHAS
   Solution. GRUNGY, 6
   (d) ARENA
   Solution. RIVER, 17
   (e) FAKE
   Solution. TOYS, 14
   (f) LATTE
   Solution. FUNNY, 20
   (g) LAYOUT
   Solution. FUSION, 20
   (h) MEET
   Solution. WOOD, 10
   (i) OVALS
   Solution. HOTEL, 19

4. Suppose that you have an alphabet of 26 letters. A simple substitution cipher is the one we discussed in class - we encrypt letter by letter.

   (a) How many possible simple substitution ciphers are there?
   Solution. A can be sent to any of $A, B, \cdots, Z$, giving 26 choices. B can be sent to any of the alphabets uncovered, giving 25 choices. Continuing, we see that there are $26! \sim 4.0 \times 10^{26}$ simple substitution ciphers.
   (b) How many simple substitution ciphers are there with A fixed?
   Solution. If A is sent to A, same analysis says that B has 25 choices (B all the way up to Z), C has 24 choices and so on - the answer is $25! \sim 1.6 \times 10^{25}$.
   (c) How many simple substitution ciphers are there with A and B fixed?
   Solution. Similar as the two parts above: answer is $24! \sim 6.2 \times 10^{23}$.
   (d) How many simple substitution ciphers are there with A or B fixed?
   Solution. We can add up those that fix A, and those that fix B, but there will be a double counting of those that fix A and B, so we need to subtract that once. So the answer is $25! + 25! - 24!$.
   ⋆ (e) How many simple substitution ciphers are there with no letter fixed?
   Solution. This is the *derangement problem*. The analysis is similar to the last part, and is formalized by Principle of Inclusion-Exclusion. The answer is

$$26! - 26 \cdot 25! + \binom{26}{2} \cdot 24! - \binom{26}{3} \cdot 23! + \cdots + \binom{26}{26} \cdot 0!$$

   If you google about derangement problem, you will find many websites explaining why the answer is as above.

   Hint: to get started on the problem, you may want to work out the case of 4 letters first.

5. Substitution cipher 2 Each of the following messages has been encrypted using a simple substitution cipher. Decrypt them.

   (a) (This one has the space preserved.)

```
AUHC MVKFC V BYZUGC V IZMC CJ GUMBZYAZD UKUVM.
```

VC HZZGZB CJ GZ V HCJJB PD CFZ VYJM KUCZ AZUBVMK
CJ CFZ BYVWZ UMB OJY U IFVAZ V TJNAB MJC ZMCZY OJY
CFZ IUD IUH PUYYZB CJ GZ.

Solution. Last night I dreamt I went to Manderley again. It seemed to me I stood by the iron gate leading to the drive and for a while I could not enter for the way was barred to me.

⋆ (b) The flora.

KZRNK GJKIP ZBOOB XLCRG BXFAU GJBNG RIXRU XAFGJ
BXRME MNKNG BURIX KJRXR SBUER ISATB UIBNN RTBUM
NBIGK EBIGR OCUBR GLUBN JBGRL SJGLN GJBOR ISLRS
BAFFO AZBUN RFAUS AGGBI NGLXM IAZRX RMNVL GEANG
CJRUE KISRM BOOAZ GLOKW FAUKI NGRIC BEBRI NJAWB
OBNNO ATBZJ KOBRC JKIRR NGBUE BRINK XKBAF QBROA
LNMRG MALUF BBG

Hint: The frequency table is

	B	R	G	N	A	I	U	K	O	J	L	X	M	F	S	E	Z	C	T	W	P	V	Q
Freq	32	28	22	20	16	16	14	13	12	11	10	10	8	8	7	7	6	5	3	2	1	1	1

The most frequent bigrams are: NG and RI (7 times each), BU (6 times), BR (5 times), and GL, OA, IN, XR, BN, KI, GR, GJ, GB (4 times).

Here's a frequency table for alphabets and digrams in English: (Reference: here and here.)

Alphabets Frequency			
e	12.7 %	m	2.4 %
t	9.1 %	w	2.4 %
a	8.2 %	f	2.2 %
o	7.5 %	g	2.0 %
i	7.0 %	y	2.0 %
n	6.7 %	p	1.9 %
s	6.3 %	b	1.5 %
h	6.1 %	v	1.0 %
r	6.0 %	k	0.8 %
d	4.3 %	j	0.2 %
l	4.0 %	x	0.2 %
c	2.8 %	q	0.1 %
u	2.8 %	z	0.1 %

Bigrams Frequency			
th	1.52 %	en	0.55 %
he	1.28 %	ed	0.53 %
in	0.94 %	to	0.52 %
er	0.94 %	it	0.50 %
an	0.82 %	ou	0.50 %
re	0.68 %	ea	0.47 %
nd	0.63 %	hi	0.46 %
at	0.59 %	is	0.46 %
on	0.57 %	or	0.43 %
nd	0.56 %	ti	0.34 %
ha	0.56 %	as	0.33 %
es	0.56 %	te	0.27 %
st	0.55 %	et	0.19 %

Solution. I was, I think, well educated for the standard of the day. My sister and I had a German governess, a very sentimental creature. She taught us the language of flowers, a forgotten study nowadays, but most charming. A yellow tulip for instance means hopeless love, while a china aster means I die of jealousy at your feet.

6. Prove the following by modifying Euclid's proof.

(a) There are infinitely many primes congruent to 3 mod 4. (Hint: Suppose that there are only finitely many such primes, and they are $p_1, \cdots, p_k$. Consider $N = 4p_1 \cdots p_k - 1$.)

Solution. Suppose not. Let $p_1, \cdots, p_k$ be all the primes congruent to 3 mod 4. Consider $N = 4p_1 \cdots p_k - 1$. Since $N \equiv 3 \bmod 4$, N must have a prime factor $p \equiv 3 \bmod 4$. This p is not among $p_1, \cdots, p_k$, since $p_1, \cdots, p_k$ do not divide N. Contradiction.

(Why must N have a prime $p \equiv 3 \bmod 4$? This is because N is an odd number, so its prime factors must be congruent to either 1 or 3 mod 4. If N does not have a prime $p \equiv 3 \bmod 4$, all its prime factors are congruent to 1 mod 4, forcing N to be congruent to 1 mod 4. Contradiction)

⋆ (b) Prove that there are infinitely many primes congruent to 1 mod 4.

Solution. See Homework 4, Question 4.

7. Check that multiplication modulo m is well-defined. In other words, prove that if $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$, then
$$ab \equiv a'b' \bmod m.$$

Solution. Let $a' = xm + a$, and $b' = ym + b$. Then
$$a'b' = (xm + a)(ym + b) = xym^2 + aym + xbm + ab = m(xym + ay + xb) + ab \equiv ab \bmod m$$

8. (a) Find $100 \cdot 101 \cdot 102 \cdot 103 \bmod 99$.
Solution. $100 \cdot 101 \cdot 102 \cdot 103 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \bmod 99 \equiv 24 \bmod 99$
(b) Find $100 \cdot 99 \cdot 98 \cdot 97 \bmod 101$.
Solution. $100 \cdot 99 \cdot 98 \cdot 97 \equiv (-1) \cdot (-2) \cdot (-3) \cdot (-4) \bmod 101 \equiv 24 \bmod 101$
(c) Find the last digit of 2^{2015}.
Solution. We need to find $2^{2015} \bmod 10$. Note that $2^2 \equiv 4 \bmod 10$, $2^3 \equiv 8 \bmod 10$, $2^4 = 16 \equiv 6 \bmod 10$, $2^5 = 32 \equiv 2 \bmod 10$, so the unit digit repeats itself as you add 4 to the exponent. Since $2015 \equiv 3 \bmod 4$, the last digit is $2^3 = 8$.
(d) Given an integer n in its decimal expansion $\overline{a_k a_{k-1} \cdots a_0}$, show that
$$n \equiv a_k + a_{k-1} + \cdots + a_0 \bmod 9$$
For example, this means that
$$1234 \equiv 1 + 2 + 3 + 4 \bmod 9 \equiv 10 \bmod 9 \equiv 1 \bmod 9.$$
In particular, find the remainder of
$$\underbrace{20152015\cdots2015}_{\text{repeating 2015 times}}$$
when divided by 9.
Solution.
$$\begin{aligned} n &= a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \cdots + a_0 \\ &\equiv a_k \cdot 1^{k-1} + a_{k-1} \cdot 1^{k-2} + \cdots + a_0 \bmod 9 (\text{since } 10 \equiv 1 \bmod 9) \\ &\equiv a_k + a_{k-1} + \cdots + a_0 \bmod 9 \end{aligned}$$
Thus,
$$\underbrace{20152015\cdots2015}_{\text{repeating 2015 times}} \equiv \underbrace{2+0+1+5+2+0+1+5+\cdots}_{\text{repeating 2015 times}} \bmod 9 \equiv 2015\cdot(2+0+1+5) \bmod 9 \equiv (2+0+1+5)^2 \bmod 9 \equiv 1 \bmod 9$$
(e) Can you design a divisibility test for 11? In other words, given an integer n in its decimal expansion $\overline{a_k a_{k-1} \cdots a_0}$, figure out a way to quickly find $n \bmod 11$.
Solution. We can do alternating sums of digits of n, starting from the unit digit. For example,
$$1234 \equiv 4 - 3 + 2 - 1 \equiv 2 \bmod 11$$

9. Let m be a positive integer, not necessarily a prime. If $ab \equiv 0 \bmod m$, does it imply $a \equiv 0 \bmod m$ or $b \equiv 0 \bmod m$? If it is true, prove it; if not, give a counterexample.
Solution. This is not true, whenever m is not a prime. For example, consider $m = 6$. Then $a = 2$, $b = 3$ is a counterexample. In general, take any composite m, and take any non-trivial factorization of m as your a, b would give you a counterexample.

10. Which problem do you like the best/the least? Why?

Homework 2

Reference for today's lecture: Chapter 4.2, 4.3, 5.1-5.3 of textbook.

1. Compute the greatest common divisor of the following using Euclidean algorithm. Show your work.
   (a) GCD(7, 17).
   Solution. Do repeated division:
   $$17 = 2 \cdot \boxed{7} + \boxed{3}$$
   $$\boxed{7} = 2 \cdot \boxed{3} + \boxed{1}$$
   $$\boxed{3} = 3 \cdot \boxed{1} + 0$$
   Thus the GCD is 1. (The last remainder before 0)
   (b) GCD(4, 50).
   Solution. 2
   (c) GCD(98, 35).
   Solution. 7
   (d) GCD(123, 234).
   Solution. 3
   (e) GCD(201, 335).
   Solution. 67

2. Find
   (a) The multiplicative inverse of 7 in $((\mathbb{Z}/17\mathbb{Z})^*, \times)$.
   Solution. 5. This can be seen by inspection, since $5 \cdot 7 = 35 \equiv 1 \bmod 17$. Or we can use Extended Euclidean Algorithm to reverse the GCD(7,17) calculation done in 1(a). Going from the second-to-the-last line to the top:
   $$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (17 - 2 \cdot 7) \text{ (back substituting 3 from the line before)} \\ &= 7 - 2 \cdot 17 + 4 \cdot 7 \\ &= 5 \cdot 7 - 2 \cdot 17 \end{aligned}$$
   Thus $5 \cdot 7 = 1 + 2 \cdot 17 \equiv 1 \bmod 17$, showing that 5 is the inverse.
   (b) The multiplicative inverse of 7 in $((\mathbb{Z}/37\mathbb{Z})^*, \times)$.
   Solution. 16
   (c) The multiplicative inverse of 7 in $((\mathbb{Z}/101\mathbb{Z})^*, \times)$.
   Solution. 29

3. Find an integer solution to the given linear diophantine equation, or show that there are no solutions.
   (a) $7x + 17y = 1$.
   Solution. Check GCD(7,17) = 1, which divides the right hand side, so this has a solution. To find an explicit solution, use Extended Euclidean Algorithm to reverse the GCD(7,17) calculation. We did this in 3(a), and get
   $$1 = 5 \cdot 7 - 2 \cdot 17$$
   Thus a solution is $x = 5$, $y = -2$.
   (b) $7x + 37y = 2015$.
   Solution. Check GCD(7,37) = 1, which divides right hand side 2015, so this has a solution. To find an explicit solution, first use Extended Euclidean Algorithm to find one solution for $7x + 37y = 1$. For example, $x = 16$, $y = -3$ works. Then multiply both sides of $7x + 37y = 1$ by 2015 to get
   $$7(2015x) + 37(2015y) = 2015$$
   so one solution is $x = 2015 \cdot 16 = 32240$, $y = -6045$.

(c) $7x + 37y + 59z = 2015$.

Solution. We knew already that GCD(7,37) = 1, so we may as well set $z = 0$ and re-use our solution from last part. So $x = 32240$, $y = -6045$, $z = 0$.

(d) $91x + 221y = 15$.

Solution. Check GCD(91, 221) = 13, which does NOT divide right hand side 15. Thus there is no solution, since left hand side is always a multiple of 13, while right hand side is not.

⋆ (e) How would you find an integer solution to $ax + by = c$ for given integer a, b, c in general? What about $ax + by + cz = d$ for given integer a, b, c, d?

Solution. Two variable case: check whether $GCD(a, b)$ divides c. If not, no solution. If yes, use Extended Euclidean Algorithm.

Three variable case: check whether $GCD(a, b, c)$ divides d. If not, similarly there is no solution. If yes, it is possible to do extended Euclidean Algorithm repeatedly to get a solution.

Let $GCD(a, b) = g$. Then

$$GCD(g, c) = GCD((a, b), c) = GCD(a, b, c)$$

Since we assumed that $GCD(a, b, c)|d$ so that a solution is possible, we also know that $GCD(g, c)|d$ thus we can solve $gw + cz = d$ in w and z. After finding one solution for w, z, solve $ax + by = gw$, which definitely has a solution since $GCD(a, b) = g$ divides gw. Substituting the solution of x, y back into $gw + cz = d$, we get a solution of

$$ax + by + cz = d$$

4. Solve the following congruences:

(a) $7x \equiv 1 \bmod 17$.

Solution. $x \equiv 5 \bmod 17$. This is because we knew from Question 3 that the multiplicative inverse of $7 \bmod 17$ is $5 \bmod 17$, so we can just multiply $5 \bmod 17$ on both sides to get

$$5(7x) \equiv 5 \bmod 17$$
$$x \equiv 5 \bmod 17$$

(b) $7x \equiv 2015 \bmod 37$.

Solution. $x \equiv 13 \bmod 37$

(c) $7x \equiv 2 \bmod 101$.

Solution. $x \equiv 58 \bmod 101$

(d) $x^2 \equiv 1 \bmod 5$.

Solution. $x \equiv \pm 1 \bmod 5$

This is because $x^2 - 1 \equiv 0 \bmod 5$, so

$$(x - 1)(x + 1) \equiv 0 \bmod 5$$

Since 5 is a prime, if $(x - 1)$ and $(x + 1)$ multiply to be a multiple of 5, either one of them is $0 \bmod 5$, so either $x \equiv 1 \bmod 5$ or $x \equiv -1 \bmod 5$.

(e) $x^2 \equiv 1 \bmod 6$.

Solution. $x \equiv \pm 1 \bmod 6$. One can brute force it by trying $0 \bmod 6, 1 \bmod 6$ up to $5 \bmod 6$ directly.

Alternatively, one can also follow the same approach for (d): $x^2 - 1 \equiv 0 \bmod 6$, and $(x-1)(x+1) \equiv 0 \bmod 6$.

But as 6 is NOT a prime, we cannot conclude that $x \equiv \pm 1 \bmod 6$. We will need to see when two numbers multiply to be 0 mod 6. There are a few cases, (other than either one of them is 0)

$$2 \cdot 3, 3 \cdot 2, 4 \cdot 3, 3 \cdot 4$$

So other than either one of $(x - 1), (x + 1)$ is zero (which gives you $x \equiv \pm 1 \bmod 6$, you have to check the following four cases

$$\begin{cases} x - 1 \equiv 2 \bmod 6 \\ x + 1 \equiv 3 \bmod 6 \end{cases}, \begin{cases} x - 1 \equiv 3 \bmod 6 \\ x + 1 \equiv 2 \bmod 6 \end{cases}, \begin{cases} x - 1 \equiv 4 \bmod 6 \\ x + 1 \equiv 3 \bmod 6 \end{cases}, \begin{cases} x - 1 \equiv 3 \bmod 6 \\ x + 1 \equiv 4 \bmod 6 \end{cases}$$

None of these four cases give a solution.

5. For each a in $\mathbb{Z}/7\mathbb{Z}$, determine whether there is a positive integer k such that
$$a^k \equiv 1 \bmod 7$$
Each time there is such a k, find the smallest such k. What is the smallest number k that works for all these a's?
Do the same with 7 replaced with 8.

Solution. Just brute force and check.
For 7: $a = 0$: none. $a = 1 : 1$, $a = 2 : 3$, $a = 3 : 6$, $a = 4 : 3$, $a = 5 : 6$, $a = 6 : 2$. Smallest k for all a's is 6.
For 8: $a = 0, 2, 4, 6$: none. $a = 1 : 1$, $a = 3 : 2$, $a = 5 : 2$, $a = 7 : 2$. Smallest k for all a's is 2.

6. Let $p > 2$ be a prime. $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is called a *quadratic residue* modulo p, if there exists some x such that
$$x^2 \equiv a \bmod m.$$
Otherwise it is called a *quadratic non-residue*.
For example, if $m = 5$, then as $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 4 \bmod 5, 4^2 = 16 \equiv 1 \bmod 5$, we see that $1, 4$ are quadratic residues mod 5, while $2, 3$ are the quadratic non-residues.
(a) Find all the quadratic residues modulo 7. Do the same for 11.
(b) How many quadratic residues modulo 7 are there? Same question for 11.
⋆ (c) Do the same for some other primes p other than 2. Make a guess for the number of quadratic residues modulo p. Try to prove your guess.

Solution.
(a) Just brute force. 7: 1, 4, 2. 11: 1, 4, 9, 5, 3.
(b) 7: 3. 11: 5.
(c) $\frac{p-1}{2}$. Beyond scope of class as of now, but should be do-able after square test. Main point is $(\mathbb{Z}/p\mathbb{Z})^*$ is generated by one element g, i.e. every every element is uniquely g^k for some unique $k \bmod p-1$. If this k is even, $g^k \bmod p$ is a square/quadratic residue; if this k is odd, $g^k \bmod p$ is not a square/is quadratic non-residue. Since there are $\frac{p-1}{2}$ even (odd) numbers from 1 to $p-1$, there are $\frac{p-1}{2}$ quadratic residues (non-residues) mod p.

7. (a) Suppose that $g^a \equiv 1 \bmod m$, and $g^b \equiv 1 \bmod m$, show that
$$g^{gcd(a,b)} \equiv 1 \bmod m.$$
⋆ (b) Fix $g \bmod m$. Let d be the smallest positive integer $g^d \equiv 1 \bmod m$. If we also know that $g^a \equiv 1 \bmod m$, prove that $d|a$.

Solution. Extended Euclidean Algorithm/Bezout's identity shows that there are some integers u, v such that
$$ua + vb = gcd(a, b)$$
Thus,
$$g^{gcd(a,b)} \equiv g^{ua} \cdot g^{vb} \bmod m \equiv (g^a)^u \cdot (g^b)^v \bmod m \equiv 1 \cdot 1 \bmod m \equiv 1 \bmod m$$

8. The following were encrypted by Vigenere cipher. Find the key and decrypt the message.
(a)
```
MGODT BEIDA PSGLS AKOWU HXUKC IAWLR CSOYH PRTRT UDRQH CENGX UUQTU HABXW DGKIE
KTSNP SEKLD ZLVNH WEFSS GLZRN PEAOY LBYIG UAAFV EQGJO EWABZ SAAWL RZJPV FEYKY
GYLWU BTLYD KROEC BPFVT PSGKI PUXFB UXFUQ CVYMY OKAGL SACTT UWLRX PSGIY YTPSF
```

RJFUW IGXHR OYAZD RAKCE DXEYR PDOBR BUEHR UWCUE EKFIC ZEHRQ IJEZR XSYOR TCYLF
EGCY

Solution. It is to be questioned whether in the whole length and breadth of the world, there is a more admirable spot for a man in love to pass a day or two than the typical English village. It combines the comforts of civilization with the restfulness of solitude in a manner equalled by no other spot except the New York.

(b) WVKKUURFFESHUJFGSVEQUPSYTXRAWVKUXHSQKUURYYXBDZRGPS
GQWTJNLRJHBDBJUXDDNHWTAKDBOQUZFOWWTJIUMVWCMUOVKMLG
WVKGZXRECLVOGRKQCUWZLBMCXHNHYFWKQQKCLSTFFESHOQUDBJ
RKFFESHOQUWSDWTLBKWSKQHNQKQHAUMVQNRZGUGGSIUMVWSJOT
FWKQHHUESHODBKWKUCMOMVKWIVCKSTBGSCRHCTVYRZJLSXVLRI
TGZKSUCYHHZDYWCTHTHOXFUVSZWOHUESHLHYWTVQXLDZLCTDXD
WYLBMYOQUSHUOSSBBKGVOQZKFKHGQQOHBZZGQUADUKVJHAUWWI
VOHFUJZESVOFGDBJUXHSQHNHYFVUOOXVCKCFCAORUSGGGQQOHB
ZUXHSQRKFFESHKGZKSRHNHFOOTJIGJSYPEHXDBYOOZLBMHNHMU
SKNGQRFCSSOXLBMHNHZKFKHOQGIUWVWWUQGLBWVKHCHBZLSZKI
HBZXFEKUUZJCLQUPDAWSXBKWKUUYYAKVGGJSYOXHJLUOWOROMH
BIUMVWSJCTHNHYHBJLBMGOGSDBJRKFFESHKGUQZKSUSIHWBLBM
GOGSXGOQUFFESHUJFGSVOFYHFBLQKVGQRDZMRFOWVSVGOUUUWZ
KAYOXHSDHNHAGWWIDZWSIKBOTIKVUUXXZKVZKOZOVSZEOFFESH
UJFGSVOFYHFBLQKHUOPSYVOMH

9. The transposition cipher aims to rearrange the letters in some way, rather than doing substitution of letters. One example is the rail-fence cipher, which encrypts encrypts the message "cryptographyiscool" by writing it in a zig-zag way

c . y . t . g . a . h . i . c . o .
. r . p . o . r . p . y . s . o . l

then read off the rows, giving us the ciphertext CYTGAHICORPORPYSOL.

(a) Encrypt a quick brown fox jumps over the lazy dog.
Solution. AUCBONOJMSVRHLZDGQIKRWFXUPOETEAYOO

(b) Decrypt YSHSSORCETIICRET.
Solution. yes this is correct

(c) Another example is the columnar cipher. Suppose that the key is 5, then we will write our message "cryptographyiscool" in five columns,

CRYPT
OGRAP
HYISC
OOL..

and read it off vertically from left to right to get the ciphertext COHORGYOYRILPASTPC. Without knowing the key, suggest a way to decipher the message.
Solution. Write the ciphertext in columns of rectangles of various lengths. Try to read horizontally and see if any of them make sense.

(d) Explain whether frequency analysis is useful for deciphering transposition ciphers.
Solution. Shouldn't be useful, because the position of the letters are all changed.

⋆ 10. The affine cipher is defined as follows. Let the plaintext space CP be $\{a, \cdots, z\}$, the ciphertext space $\mathcal{C}$ be $\{A, \cdots, Z\}$, both identified with $(\mathbb{Z}/26\mathbb{Z}, +)$ by identifying

$$a, A \to 0 \bmod 26 \text{ and } b, B \to 1 \bmod 26 \text{ and } c, C \to 2 \bmod 26 \cdots$$

Let the key space $\mathcal{K}$ be the set of pair of numbers (k_1, k_2), so that k_1 lies in $((\mathbb{Z}/26\mathbb{Z})^*, \times)$, and k_2 lies in $(\mathbb{Z}/26\mathbb{Z}, +)$.

The encryption of a message m is then

$$e_{(k_1,k_2)}(m) = k_1 m + k_2 \bmod 26$$

(a) Encrypt the message "cryptographyiscool" with the key $(5, 1)$.
Solution. Essentially we are encrypting by $m \to 5m + 1 \bmod 26$, where we identify $a \to 0$, $b \to 1$ and so on. LIRYSTFIBYKRPNLTTE

(b) Explain in words, why encryption with a key $(1, k_2)$ is the same as the shift cipher with key k_2.
Solution. We are encrypting by $m \to 1 \cdot m + k_2 \bmod 26 = m + k_2 \bmod 26$. This is precisely the shift cipher.

(c) Explain how one can decode the affine cipher given the key (k_1, k_2).
Solution. We are given $c \equiv k_1 m + k_2 \bmod 26$, and we want to solve for m. So

$$\begin{aligned} c &\equiv k_1 m + k_2 \bmod 26 \\ k_1 m &\equiv c - k_2 \bmod 26 \\ m &\equiv k_1^{-1}(c - k_2) \bmod 26 \end{aligned}$$

The last step is possible because k_1 was assumed to be in $(\mathbb{Z}/26\mathbb{Z})^*$, ensuring that the inverse exists.

(d) If Alice and Bob send messages to each other using affine cipher, how can Eve crack the message?
Solution. This is still a substitution cipher, so it's prone to frequency analysis. Alternatively, there are only $\phi(26) \cdot 26 = 12 \cdot 26 = 312$ possibilies of affine cipher, making a case-by-case check easy enough.

Homework 3

1. The order of a in $(\mathbb{Z}/m\mathbb{Z}, +)$ is the smallest positive integer n such that $na \equiv 0 \bmod m$. Compute the order of a in the following cases.
   (a) $a = 2$, $m = 5$.
   Solution. 5, because
   $1 \cdot 2 \equiv 2 \bmod 5$, $2 \cdot 2 \equiv 4 \bmod 5$, $3 \cdot 2 \equiv 1 \bmod 5$, $4 \cdot 2 \equiv 3 \bmod 5$, $5 \cdot 2 \equiv 0 \bmod 5$
   So 5 is the first time that sends 2 back to 0.
   (b) $a = 2$, $m = 6$.
   Solution. 3
   (c) $a = 3$, $m = 6$.
   Solution. 2
   (d) $a = 3$, $m = 17$.
   Solution. 17
   In what case(s) above is a a generator of $(\mathbb{Z}/m\mathbb{Z}, +)$?
   Solution. (a), (d).
   $\mathbb{Z}/m\mathbb{Z}$ has m elements since there are m remainders, so generator in this case means that the order equals m.

2. Compute the order of a in $\mathbb{F}_p^*$ under multiplication:
   (a) $a = 2$, $p = 5$.
   Solution. 4, because
   $2^1 \equiv 2 \bmod 5, 2^2 \equiv 4 \bmod 5, 2^3 \equiv 3 \bmod 5, 2^4 \equiv 1 \bmod 5$
   (b) $a = 2$, $p = 7$.
   Solution. 3
   (c) $a = 3$, $p = 7$.
   Solution. 6
   (d) $a = 2$, $p = 11$.
   Solution. 10
   In what case(s) above is a a primitive root mod p?
   Solution. (a),(c),(d). Primitive roots are those whose order is $p - 1$.

3. Compute the following,
   (a) $2^{60} \bmod 7$.
   Solution. 1. Fermat's little theorem says $2^6 \equiv 1 \bmod 7$. Raise it to 10th power.
   (b) $3^{60} \bmod 7$.
   Solution. 1. Same as last part.
   (c) $3^{60} \bmod 8$.
   Solution. 1. Fermat's little theorem CANNOT be applied since 8 is not a prime. But $3^2 \equiv 1 \bmod 8$ by direct computation. Raise it to 30th power.
   (d) $3^{60} \bmod 9$.
   Solution. 0, since 3^2 is already congruent to $0 \bmod 9$.
   (e) $2^{96} \bmod 97$. (Hint: 97 is a prime.)
   Solution. 1, by Fermat's little theorem.

4. Let $p > 2$ be a prime, and g be a primitive root of p. Recall that $a \bmod p$ is a quadratic residue if there is some x such that $x^2 \equiv a \bmod p$, i.e. a is a square mod p.
   Prove that $a = g^k \bmod p$ in $\mathbb{F}_p^*$ is a quadratic residue modulo p if and only if k is even.
   Solution. If k is even, $a = g^k = (g^{k/2})^2$ is a square mod p.
   If a is a quadratic residue mod p, let $a \equiv x^2 \bmod p$ for some x. Since g is a primitive root, $x = g^m$ for some m. Then $a \equiv g^{2m} \bmod p$, so $k \equiv 2m \bmod p - 1$ is even, since $p - 1$ is even.
5. Let $p > 2$ be a prime, and a in $\mathbb{F}_p^*$.

(a) Prove that $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.
Solution. Fermat's little theorem gives $a^{p-1} \equiv 1 \bmod p$. Thus,

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \bmod p$$
$$\left(a^{\frac{p-1}{2}}\right)^2 - 1 \equiv 0 \bmod p$$
$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p$$

Since p is a prime, either the first or second term equals 0, meaning that $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.

(b) If g is a primitive root mod p, show that $g^{\frac{p-1}{2}} \equiv -1 \bmod p$. (Hint: By part (a), it is either 1 or -1. Can it be 1?)
Solution. $g^{\frac{p-1}{2}}$ cannot be 1, since by definition g has order $p-1$, i.e. $g^k \not\equiv 1 \bmod p$ for any $0 < k < p-1$. This forces $g^{\frac{p-1}{2}} \equiv -1 \bmod p$.

⋆ (c) Prove Euler's criterion:

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \bmod p & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 \bmod p & \text{if } a \text{ is not a quadratic residue modulo } p \end{cases}$$

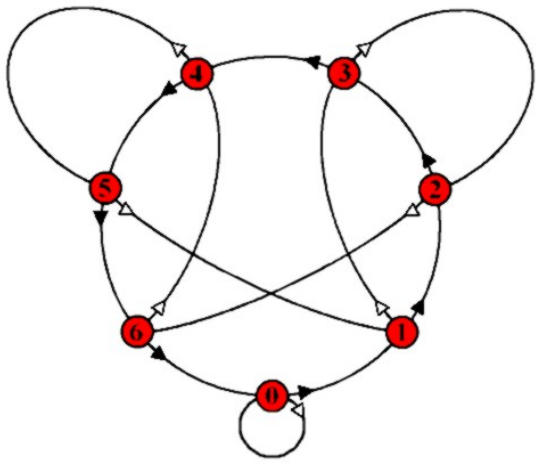
(Hint: Use primitive roots, and Fermat's little theorem)
Solution. Use the last question. If a is a quadratic residue mod p, write $a \equiv g^k \bmod p$ for some even k. Then

$$a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} \bmod p \equiv (g^{k/2})^{p-1} \bmod p \equiv 1 \bmod p$$

where the last equality comes from Fermat's little theorem.
If a is a quadratic residue mod p, then $a \equiv g^k \bmod p$ for some ODD p. Similar calculations show that

$$a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \bmod p \equiv -1 \bmod p$$

6. Here is a divisibility test for 7. Write down a number n. Start at the small white node at the bottom of the graph. For each digit d in n, follow d black arrows in a succession, and as you move from one digit to the next, follow 1 white arrow.



For example, if $n = 325$, follow 3 black arrows, then 1 white arrow, then 2 black arrows, then 1 white arrow, and finally 5 black arrows.

The node you end up with correspond to $n \bmod 7$. For 325, you should land at 3, meaning that $325 \equiv 3 \bmod 7$.

(a) Explain why the test works.

Solution. Black arrow corresponds to adding 1 mod 7. White arrow corresponds to multiplying 10 mod 7, which is what you need as you move across digits.

(b) Can you formulate a similar test for 9?

Solution. Draw 9 nodes corresponding 0, 1, 2, ..., 8, corresponding to $0 \bmod 9, \cdots, 8 \bmod 9$. Black arrow adds 1, so it's like a cyclic loop as before. White arrow multiplies by $10 \equiv 1 \bmod 9$, so from each node there is a white arrow pointing back to itself.

7. The following are encrypted using either Columnar cipher, Vigenere cipher, or substitution cipher. Figure out which is which. Crack them too if you like. You can assume that any Columnar cipher has a key of at most 3 characters.

(a)
```
HUKDOPSLPDHZAHSRPUNAOLPKLHVMHJABHSSFSVZPUNWLLAHO
PATLHNHPUHUKPYLHSPGLKOVDTBJOPKVUADHUAOPTAVKPLHUK
PAZUVAHIVBAAOLZWVUZVYZHUKPAZUVAHIVBADOHADPSSOHWW
LUDOLUDLNLAOVTLHUKPAZUVAQBZAAOHAPKVUADHUAAVILHSV
   ULPAZOPTPKVUVADHUAAVSVZLAOLIVFDPAOAOLIYLHK
```

Solution. And while I was talking, the idea of actually losing Peeta hit me again and I realized how much I don't want him to die. And it's not about the sponsors. And it's not about what will happen when we get home. And it's not just that I don't want to be alone. It's him. I do not want to lose the boy with the bread.

(b)
```
OVPUIMFVLOFLQKQZZDZBPVWQGSXOKPHRGGRYOSCDPXSMXIMZ
XQGGKAVJPQSFWTXYPZWLTOCYWZZRHECIICOYVVMWJXYPJPYS
UCXNDCRFMPCROVPRRXMKPJDLUWQZDHPHSVXAQFFZHZKSSKRK
OGDLROSKAZUCHEFGCROVPUMZVZFNSWIAQSMXIZZROECDXOVT
QKMZZDZPFWERHVKVZWLXIOJFZFPOCMZLVFMNKEZQVMCOEVEH
        SURJIQUSYAVMCOEVEXZZPVBEHHFCBGJK
```

Solution. There are strange likenesses between us, after all. Even you must have noticed. Both half-bloods, orphans, raised by Muggles. Probably the only two Parselmouths to come to Hogwarts since the Great Slytherin himself. We even look something alike ... but after all, it was merely a lucky chance that saved you from me. That's all I wanted to know.

(c)
```
EOIWAEEURAYLHEAPARKONARTIOEEEHTPNEOOOIIREEEESRPR
OHNPMEFRVAATPNOAWAIOAENOTTEWNOERHEOWNWKGNEETTLNW
BNERDOOLIOACLEIARVWHTHRRNFNAFQNSOPTEOAPURUSPDSEL
NNNNDEHHENUFMSOEADQSFRABUTLRISTSELYHHEMNAGNNCDDL
HTRAONRUTPNAOOIFEXPHAMEAEGTNUNMEOFCAAPRNREIIHOAI
DMESRUTEFAEPNTOLTCTAWGAYCVICWNEOWTTCMSNPTRUTOEIR
GOYOSAEERDSEOCPYSACTTATDAHESLGASHHESWRNICCTALOYS
              IRUEPCPTNEHLRAMAIDTNEU
```

Solution. A friend of mine was a frequent user of a pay telephone at a popular truck stop, and was greatly inconvenienced when the phone went out of commission.Repeated requests for repair brought only promises.After several days, the phone company was again contacted and told that there was no longer a rush.The phone was now working fine–except that all money was being returned upon completion of each call.A repairman arrived within the hour!

Homework 4

Reference for today's lecture: Chapter 6.3, 9.3 of textbook. For the graph cryptosystem, see http://csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf

1. For $p > 2$ prime, we always have $gcd(2, p) = 1$, so Fermat's little theorem says that
$$2^{p-1} \equiv 1 \bmod p$$
Try to compute $2^{560} \bmod 561$. Is 561 a prime?
Solution. $2^{560} \equiv 1 \bmod 561$. This can be done by brute force:
$$\begin{aligned} 2^{560} &\equiv (2^{10})^{56} \bmod 561 \\ &\equiv 1024^{56} \bmod 561 \\ &\equiv (-98)^{56} \bmod 561 \\ &\equiv (98^2)^{28} \bmod 561 \\ &\equiv 67^{28} \bmod 561 \\ &\equiv (67^2)^{14} \bmod 561 \\ &\equiv 1^{14} \bmod 561 \\ &\equiv 1 \bmod 561 \end{aligned}$$
$561 = 3 \times 11 \times 17$ is not a prime. The significance is that the converse of Fermat's little theorem is false.

2. Let p be a prime, and a be an integer. Define the Legendre symbol
$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a \\ 1 & \text{if } a \text{ is a square/quadratic residue modulo } p \\ -1 & \text{if } a \text{ is not a square/quadratic residue modulo } p \end{cases}$$
Compute
   (a) Compute $\left(\frac{3}{5}\right)$, $\left(\frac{7}{5}\right)$, $\left(\frac{11}{5}\right)$ and $\left(\frac{13}{5}\right)$.
   Solution. -1, -1, 1, -1. This can be computed by brute force,
   $$1^2 \equiv 1 \bmod 5, 2^2 \equiv 4 \bmod 5, 3^2 \equiv 4 \bmod 5, 4^2 \equiv 1 \bmod 5$$
   So only those congruent to 1 or 4 mod 5 has Legendre symbol being 1. Those congruent to 2 or 3 mod 5 has Legendre symbol -1.
   (b) Compute $\left(\frac{5}{3}\right)$, $\left(\frac{5}{7}\right)$, $\left(\frac{5}{11}\right)$ and $\left(\frac{5}{13}\right)$.
   Solution. -1, -1, 1, -1. Again by brute force.
   (c) Can you guess a relationship between $\left(\frac{p}{5}\right)$ and $\left(\frac{5}{p}\right)$ for a prime $p \neq 5$?
   Solution. $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$. This is (part of) quadratic reciprocity.

3. Let $p > 2$ be a prime. Show that -1 is a square modulo p if and only if $p \equiv 1 \bmod 4$.
Solution. Euler's criterion or square test says that -1 is a square mod p if and only if $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$. However, $(-1)^{\frac{p-1}{2}}$ is 1 if $p \equiv 1 \bmod 4$ and is -1 if $p \equiv -1 \bmod 4$. This proves the result.

\# 4. Fill in the details of the following proof that there are infinitely many primes $\equiv 1 \bmod 4$.
Suppose not. Assume that $p_1, \cdots, p_k$ are all the possible primes $p \equiv 1 \bmod 4$. Consider
$$N = 4(p_1 \cdots p_k)^2 + 1$$
and let $p|N$ be a prime factor.

(a) Show that p cannot be one of $p_1, \cdots, p_k$.
Solution. p_1 does not divide N because $N-1$ is already a multiple of p_1 - if N is also a multiple of p_1, then their difference 1 would be a multiple of p_1. Contradiction. Similar argument for $p_2, \cdots, p_k$.

(b) Show that -1 is a square modulo p.
Solution. $-1 \equiv 4(p_1 \cdots p_k)^2 \mod p$, since $p|N$. Thus -1 is a square mod p.

(c) Hence show that $p \equiv 1 \mod 4$. You just found a prime which is $\equiv 1 \mod 4$, yet is not among the primes $p_1, \cdots, p_k$ we listed. Contradiction.
Solution. See last question.

5. (a) Find a primitive root g for 7. For your choice of primitive root, what powers of g would give you another primitive root?
Solution. 3 or 5. Powers of g which is relatively prime to 7 - 1 = 6. Primitive root can be found by brute force.

(b) Do the same exercise with 7 replaced by 11.
Solution. Primitive roots are 2, 6, 7, 8 mod 11.

⋆ (c) Let p be a prime, and g be a primitive root. Based on the last two parts, make a guess about what k would g^k be another primitive root. Can you prove your guess? Thus try to find the number of primitive roots mod p.
Solution. g^k is a primitive root if and only if $gcd(p-1, k) = 1$. This can be shown by Bezout's identity as follows:

- If g^k is a primitive root, then for some power l we can get to g, i.e.
$$(g^k)^l \equiv g \mod p \Rightarrow g^{kl} \equiv g \mod p \Rightarrow g^{kl-1} \equiv 1 \mod p$$
Since g has order $p-1$ mod p, we know by the lemma on order in class that $p-1|kl-1$, i.e. $kl-1 \equiv 0 \mod p-1$, i.e. $kl \equiv 1 \mod p-1$. This shows that $gcd(k, p-1) = 1$.
- Conversely, if $gcd(k, p-1) = 1$, let l be the inverse of k mod $p-1$, i.e. $kl \equiv 1 \mod p-1$. Let d be the order g^k mod p, then $1 \equiv (g^k)^d \equiv g^{kd} \mod p$. The order lemma from class shows that $p-1|kd$, i.e. $kd \equiv 0 \mod p-1$. Multiplying l mod $p-1$ on both sides, we see that $d \equiv 0 \mod p-1$, i.e. $p-1|d$. But at the same time,
$$(g^k)^{p-1} \equiv (g^{p-1})^k \mod p \equiv 1^k \mod p \equiv 1 \mod p$$
So actually, $d \leq p-1$. This together with $p-1|d$ shows that $d = p-1$, i.e. g^k is a primitive root mod p.

The number of primitive roots are thus positive integers up to $p-1$ that are relatively prime to $p-1$, i.e. $\phi(p-1)$.

6. Let $p > 2$ be a prime.
(a) Find the number of elements of $(\mathbb{Z}/p^2\mathbb{Z})^*$.
Solution. $p^2 - p$. There are p^2 possibilities mod p, and we need to subtract those that has a factor in common with p^2, i.e. the multiples of p. There are p of them modulo p^2.

(b) Given that $(\mathbb{Z}/p^2\mathbb{Z})^*$ (under multiplication) has a generator, devise a test to check whether $a \mod p^2$ is a square modulo p^2.
Solution. Check whether $a^{\frac{p^2-p}{2}} \equiv \pm 1 \mod p^2$. It is 1 if and only if it is a square, and -1 if and only if it is not.

7. Find a primitive root modulo 31.
You may use a computer - Sage is free, open source mathematical software that is particularly useful in number theory. You can use it online at http://cloud.sagemath.com. See http://www.math.ucla.edu/~gschaeff/crypto/SageWorksheet.pdf for a quick introduction.
(For those who know Python, syntax of Sage is very similar to Python.)
Solution. There is a function in Sage that allows you to check whether a number is a primitive

root. 3 should work for example.

8. (a) Not every graph has a "good set" of vertices, but you can easily come up with a graph with a "good set" of vertices. How can you do that?
   Solution. Draw a group of vertices that you declare to be the good set. Draw some other random vertices. Connect them, so that for each of the "random vertices", it is connected to precisely one "good vertex". Good vertices do not connect with each other. The random vertices can have any connection you want among themselves.
   (b) Design your own "good graph". Put your name on the graph and put it on the board.
   (c) Find a friend and send him/her a message, using his/her public key (the good graph). You may encode A by 11, B by 12 and so on. For example, HI is encoded as 1819. Send them in groups of 2. For example, $HIJOHN$ would be sent by three messages 1819, 2025, 1824.
   (d) Challenge another friend to decipher your message. Hopefully that friend would be in despair trying to do so.

Homework 5

Reference for today's lecture: Chapter 4.4, Chapter 10.1-10.3 of textbook.

1. Alice has a bag of 500 candies. She just realizes that the bag was opened and a few candies were eaten. Coming from Mars, she has 13 fingers and 17 toes - a quick count shows that there are 2 candies left if she counts in groups of 13, and 3 candies left if she counts in groups of 17. Find the number of candies being eaten.
   Solution. Chinese remainder theorem suggests that you need to solve
   $$\begin{cases} x \equiv 2 \bmod 13 \\ x \equiv 3 \bmod 17 \end{cases}.$$
   Solving this system gives $x \equiv 54 \bmod 221$. Since Alice has around 500 candies originally, we add multiples of 221 to see which of them is close to 500. Now $2 \cdot 221 + 54 = 496$, so hopefully only 4 candies were eaten.

2. Find all the solutions of
   (a) $x^2 \equiv 1 \bmod 3$.
   Solution. $x \equiv \pm 1 \bmod 3$, because $(x-1)(x+1) \equiv 0 \bmod 3$ and since we are moduloing a prime, either one of $x-1$ and $x+1$ is 0 mod 3.
   (b) $x^2 \equiv 1 \bmod 7$.
   Solution. $x \equiv \pm 1 \bmod 7$. Same as above.
   (c) $x^2 \equiv 1 \bmod 21$.
   Solution. $x \equiv \pm 1, \pm 8 \bmod 21$. It is no longer true that two numbers multiply to 0 mod 21 imply either of them is 0, but we can solve the system by moduloing 3 and 7 at the same time, so that we only need to solve the system of linear equations.
   $$\begin{cases} x \equiv \pm 1 \bmod 3 \\ x \equiv \pm 1 \bmod 7 \end{cases}$$
   I am just being lazy here - there are four independent, system of linear equations to solve. Chinese remainder theorem gives the solution.
   (d) $x^2 \equiv 2 \bmod 21$.
   Solution. No solution - 21 is a multiple of 3, and $x^2 \equiv 2 \bmod 3$ already does not have solutions.

3. Find the last two digits of 7^{2015}. (Hint: $100 = 4 \cdot 25$)
   Solution. $7^{2015} \bmod 4 \equiv (-1)^{2015} \bmod 4 \equiv -1 \bmod 4$.
   $$7^{2015} \bmod 25 \equiv 49^{1007} \cdot 7 \bmod 25 \equiv (-1)^{1007} \cdot 7 \bmod 25 \equiv -7 \bmod 25$$
   Chinese remainder theorem gives $7^{2015} \equiv 43 \bmod 100$.

4. Alice and Bob decide to use the Diffie-Hellman key exchange with $p = 41$ and $g = 7$. Alice chooses $a = 14$, and Bob chooses $b = 23$. What is their shared key?
   Solution. $g^{ab} \bmod p \equiv 7^{14 \cdot 23} \bmod 41 \equiv 8 \bmod 41$

5. Bob wishes to send Alice a message encrypted with ElGamal encryption. They decide to use $p = 73$ and $g = 5$. Alice picks some a and computes the public key $g^a \equiv 49 \bmod p$. Bob chooses a random key $k = 33$ and wishes to send the message $m = 62$. What is the ciphertext he sends?
   Solution. $62 \cdot 49^{33} \bmod 73 \equiv 27 \bmod 73$.

6. The *message expansion ratio* of a cryptosystem is
   $$\text{length of ciphertext} : \text{length of plaintext}.$$
   in the worst case. For example, the Caesar cipher has a message expansion ratio of 1-to-1, because the ciphertext has the same length as the plaintext. What is the message expansion ratio of

(a) substitution cipher
Solution. 1:1
(b) Vigenere cipher
Solution. 1:1
(c) ElGamal cryptosystem?
Solution. 2:1.

7. Think about what discrete logarithm problem in $(\mathbb{Z}/m\mathbb{Z}, +)$ means, and whether it is a hard problem to solve.
Solution. It is not hard. The problem is given an additive generator $g \mod m$, and some $a \mod m$, we want to figure out a k, such that

$$kg \equiv a \mod m$$

But $k \equiv g^{-1}a \mod m$! This is merely a problem of using Euclidean algorithm, which can be done on computer fast enough.

8. Try to modify Diffie-Hellman so that it works for three people. In other words, Alice, Bob and Carol need to come up a way to have a shared secret key by communicating in a public channel.
Solution. Alice, Bob, Carol agree on prime p, primitive root g, and each choose private keys a, b, c. There are two rounds of sending messages.
- Alice sends Bob $g^a \mod p$, Bob sends Carol $g^b \mod p$, Carol sends Alice $g^a \mod p$. Now Alice can compute $g^{ac} \mod p$, Bob can compute $g^{ab} \mod p$, Carol can compute $g^{bc} \mod p$.
- Alice sends Bob $g^{ac} \mod p$, Bob sends Carol $g^{bc} \mod p$, Carol sends Alice $g^{ab} \mod p$. Now all three of them can compute $g^{abc} \mod p$, which is their shared secret key.

9. You are Barack Obama. You are fighting with another country, and you want your three commanders to launch a missile only when all of them see fit.

   The missile launching system takes a secret code and will launch the missile if the correct code is entered. If the wrong code is entered, the whole system will blow up and US is in grave trouble.

   You have the secret code, a number close to 1000. Devise a way to give some information about the code to each of the three commanders, so that any two of them won't be able to figure the actual code out, but with all three of them they can. A (unrealistic) hint: use Chinese remainder theorem!
Solution. $1001 = 7 \cdot 11 \cdot 13$. So if the secret code is x, tell commander 1 $x \mod 7$, tell commander 2 $x \mod 11$, tell commander $x \mod 17$. Also tell them the number is close to 1000.

   Any three commanders together can solve $x \mod 1001$ by Chinese Remainder Theorem. Since the number is close to 1000, they would know for sure how many multiples of 1001 to shift to get the secret code. With at most two commanders for example, they can only solve things modulo $77, 91$ or 119. These numbers are small enough comparing to 1000 that they won't be certain which shift things are, making it infeasible for them to try launching the missile. Unless, of course, they intend to blow up US..

Homework 6

Reference for today's lecture: Chapter 7, Chapter 9.4, 9.5, Chapter 10.1 - 10.3

1. Suppose that in Diffie-Hellman key exchange, instead of choosing a primitive root $g \bmod p$, we just pick a random element $g \not\equiv 0 \bmod p$, and proceed as before. What properties should g have so that the system is more secure?
   Solution. Order of g should be large. Otherwise the discrete log problem can be solved easily by listing all the powers of g and compare.

2. Suppose that Eve has an oracle to solve the discrete logarithm problem, i.e., if she tells it g and u, then the oracle tells her an x so that
   $$g^x \equiv u \bmod p$$
   How can she use this oracle to break ElGamal encryption quickly?
   Solution. Use the oracle to find the random key k. Then one can compute the twist of the message A^k directly since A is public data. Then
   $$m \equiv (mA^k)A^{-k} \bmod p \equiv c_2(A^k)^{-1} \bmod p$$

3. Determine if the following statements are right, and explain why. You can assume that all functions involved are positive.
   (a) $n^2 = O(n^3)$.
   Solution. True. Take $C = 1$.
   (b) $(\log n)^2 = O(n)$.
   Solution. True. Take $C = 1$.
   (c) If $f(n) = O(g(n))$, then $g(n) = O(f(n))$.
   Solution. False. First statement means that $g(n)$ grows faster than $f(n)$. In particular $g(n)$ can grow MUCH faster. For example, take $f(n) = 1, g(n) = n$
   (d) If $f(n) = O(g(n))$, then $e^{f(n)} = O(e^{g(n)})$.
   Solution. False. Take $f(n) = 2n$, $g(n) = n$. Then $e^{2n} = (e^n)^2$ grows faster than e^n by a lot.
   (e) If $f_1(n) = O(g_1(n))$ and $f_2(n) = O(g_2(n))$, then $(f_1 \cdot f_2)(n) = O((g_1 \cdot g_2)(n))$.
   Solution. True. Just multiply the corresponding constant in big O.

4. Assume that each of the expressions below gives the processing time $T(n)$ spent by an algorithm for solving a problem of size n. Select the dominant term(s) in n and specify the lowest Big O complexity of each algorithm.
   (a) $5 + 4n + 6n^3$.
   Solution. Dominant term $6n^3$, big O is $O(n^3)$.
   (b) $6 + n^{1.5} + 8n^3$.
   Solution. Dominant term $8n^3$, big O is $O(n^3)$
   (c) $n \log\log n + n \log n$.
   Solution. Dominant term $n \log n$, big O is $O(n \log n)$
   (d) $n(\log n)^2 + n \log n$.
   Solution. Dominant term $n(\log n)^2$, big O is $O(n(\log n)^2)$.

\# 5. (For those with programming background) The insertion sort works as follows,

```
for j ← 2 to length[A] do
    key ← A[j]
    i ← j − 1
    while i > 0 and A[i] > key do
        A[i + 1] ← A[i]
        i ← i − 1
    end whileA[i + 1] ← key
```

end for

Explain in words how insertion sort works. Analyze the number of comparisons you need for insertion sort, in terms of the input (length of array A). You can use big O notation.

Solution. Similar to rearranging cards. Take the first card. Insert the second card in the right place. Insert the third card according to ascending order, and so on.

In the worst case, when we insert the $k+1$-th card we have to shift the indices of all the known k-th cards. Thus the worst scenario in each step takes $O(k)$ steps. In total the worst scenario takes $O(1+2+\cdots+n) = O(n^2)$ steps.

6. Suppose we have a list of n sorted numbers. Devise an algorithm to look for a particular number on the list, with $O(\log n)$ comparisons.
   Solution. Do a binary search.

7. There are n points on the plane with given coordinates. We want to find the closest pair of points.
   (a) The naive algorithm computes the distance between any pair of points, and find the minimum. What is the running time complexity, if calculation of distance between one pair of points takes one unit of time?
   Solution. There are $\frac{n(n-1)}{2}$ pairs of points, thus $O(n^2)$ unit of time.
   * (b) Can you do better?
   Solution. This is the closest pair of points problem that one can look up online. It can be approached by divide-and-conquer, which would take $O(n \log n)$ time.

8. Here is an algorithm to compute $g^k \bmod n$.
   - Set $a = g$, and compute $b = g^2 \bmod n$.
   - Write k in its base 2 expansion $(x_l \cdots x_0)_2$ with $x_l = 1$, and run through $x_0, \cdots, x_{l-1}$.
     - If $x_i = 0$, set $a = a^2 \bmod n$, $b = ab \bmod n$.
     - If $x_i = 1$, set $a = a \cdot b \bmod n$, $b = b^2 \bmod n$.
   - Output a.

   (a) Explain why this works, i.e. the final output is indeed $g^k \bmod n$.
   Solution. If we track the exponent of a in each step, we can see that after the m-th step, we recover the first m-digits of the base 2 expansions.
   (b) What is the difference between this algorithm and the repeated squaring algorithm we discussed in class? More specifically, what is the computational cost of each step involved about x_i?
   Solution. The naive way of repeated squaring in class computes only a but not b. The computational cost of each step for the in-class algorithm is either one squaring or one multiplication; the cost for this algorithm is ALWAYS one squaring AND one multiplication.
   This is a naive way to defend the *timing attack* of a system. Imagine that Eve has access to the computation time of your computer. If your method of doing repeated squaring is known, then she can use the disparity of time in one squaring and one multiplication to tell apart what operation you are doing at each step - hence recovering the k herself. This is an example of a *side-channel attack*.

Homework 7

Reference for today's lecture: Chapter 10.5 - 10.6; For primality testing, see http://www.akalin.cx/intro-primality-testing

1. Using a calculator/Sage/otherwise, check by Fermat's test for $x = 2$ and 3 whether the following are primes.
   (a) 601
   Solution. 2: 1. 3: 1. Maybe.
   (b) 2047
   Solution. 2: 1. 3: 1013. Not a prime.
   (c) 294409
   Solution. 2: 1. 3: 1. Maybe.

2. Repeat the last exercise, with Miller-Rabin test instead.
   Solution. 601: pass test for 2, pass test for 3.
   2047: pass test for 2, fail test for 3 - $2046 = 2 \cdot 1023$, and $3^{1023} \equiv 1565 \not\equiv \pm 1 \mod 2047$.
   294409: fail test for 2 - $294408 = 2^3 \cdot 36801$,
   $2^{36801} \equiv 512 \not\equiv \pm 1 \mod 294409; 2^{2 \cdot 36801} \equiv 262144 \not\equiv -1 \mod 294409; 2^{2^2 \cdot 36801} \equiv 1 \not\equiv -1 \mod 294409.$
   Similarly, fail test for 3.

3. It is known that 503 is a prime with 5 being a primitive root modulo 503. Using Shank's baby-step-giant-step algorithm, find an x such that
   $$5^x \equiv 193 \mod 503$$
   Solution. $[\sqrt{503}] = 22$. Baby step would be
   $$1, 5, 25, 125, 122, 107, 32, 160, 297, 479, 383,$$
   $$406, 18, 90, 450, 238, 184, 417, 73, 365, 316, 71, 355$$
   A computer search gives that at list 22 we can find that $g^{-22 \cdot 22} h \equiv g \mod 503$, so the discrete log is $22 \cdot 22 + 1 = 485$

4. It is known that 8641 is a prime with 17 being a primitive root modulo 8641. Using Pohlig-Hellman algorithm, find an x such that
   $$17^x \equiv 2108 \mod 8641$$
   Solution. $8640 = 2^6 \cdot 3^3 \cdot 5$. So we want to calculate $k \mod 2^6$, $k \mod 3^3$, $k \mod 5$.
   We will just illustrate how to find $k \mod 3^3$. First find $k \mod 3$. Using cube test, we want to compute $2108^{\frac{8641-1}{3}} \equiv 2108^{2880} \equiv 5068 \mod 8641$, and compare to
   $$1, 17^{\frac{8641-1}{3}} \equiv 5068 \mod 8641, 17^{\frac{2(8641-1)}{3}} \equiv 3572 \mod 8641$$
   All the calculations are done by Sage. In particular it means that $k \equiv 1 \mod 3$.
   We next want to figure out $k \mod 3^2$. Write $k = 1 + 3k' \mod 3^2$, for some $k' \mod 3$. In 3^2-th power test, we want to figure out
   $$2108^{\frac{8641-1}{9}} \mod 8641 \equiv (17^k)^{\frac{8641-1}{9}} \mod 8641 \equiv 17^{\frac{8641-1}{9}} \cdot (17^{\frac{8641-1}{3}})^{k'}$$
   So k' can be found by looking at
   $$(17^{\frac{8641-1}{3}})^{k'} \equiv 2108^{\frac{8641-1}{9}} \cdot 17^{-\frac{8641-1}{9}} \equiv 1 \mod 8641$$
   So $k' \equiv 0 \mod 3$. Thus, $k \equiv 1 + 3(0) = 1 \mod 3^2$.

Finally, we figure out $k \bmod 3^3$. Write $k = 1 + 3k" \bmod 3^3$ for some $k"$ mod 3. In 3^3-th power test, we want to figure out

$$2108^{\frac{8641-1}{27}} \bmod 8641 \equiv (17^k)^{\frac{8641-1}{27}} \bmod 8641 \equiv 17^{\frac{8641-1}{27}} \cdot (17^{\frac{8641-1}{3}})^{k'}$$

So $k"$ can be found by looking at

$$(17^{\frac{8641-1}{3}})^{k'} \equiv 2108^{\frac{8641-1}{27}} \cdot 17^{-\frac{8641-1}{27}} \equiv 1 \bmod 8641$$

So $k" \equiv 0 \bmod 3$. Thus $k \equiv 1 \bmod 3^3$.

Similarly, $k \equiv 10 \bmod 2^6$ and $k \equiv 0 \bmod 5$. So we need to solve

$$\begin{cases} k \equiv 10 \bmod 2^6 \\ k \equiv 1 \bmod 3^3 \\ k \equiv 0 \bmod 5 \end{cases}$$

which gives $k \equiv 2890 \bmod 8640$.

5. Recall that *Carmichael numbers* n are integers that are not prime, but for any $(a, n) = 1$, $a^{n-1} \equiv 1 \bmod n$. They are those that would likely fool the Fermat test.
   (a) We said that 561 is a Carmichael number but we never actually checked it. Using Chinese remainder theorem, check that 561 is a Carmichael number, i.e. for all $(a, 561) = 1$,
   $$a^{560} \equiv 1 \bmod 561.$$
   (Hint: $561 = 3 \cdot 11 \cdot 17$.)
   Solution. It suffices to show that $a^{560} \equiv 1 \bmod 3$, 11 or 17.
   For 3, Note that $(a, 561) = 1$, so $(a, 3) = 1$, so by Fermat's little theorem, $a^2 \equiv 1 \bmod 3$. Then,
   $$a560 \equiv (a^2)^{280} \equiv 1 \bmod 3$$
   Similarly, one can show that $a^{560} \equiv 1 \bmod 11$ and $a^{560} \equiv 1 \bmod 17$. So $a^{560} \equiv 1 \bmod 561$.
   (b) Korselt's criterion says that a composite integer n is a Carmichael number if and only if n is odd, square-free and $p - 1|n - 1$ for all $p|n$. Use it to check that 561 is a Carmichael number. (Note: Square-free means that n is a product of distinct primes. For example, $4 = 2 \cdot 2$ is not square free, $12 = 2 \cdot 2 \cdot 3$ is not square free, but $10 = 2 \cdot 5$ is square free. Of course, any prime is squarefree.)
   Solution. $561 = 3 \cdot 11 \cdot 17$. One can check quickly that $2, 10, 16$ all divide 560.
   ⋆ (c) Prove Korselt's criterion.
   Solution. One side is easy - if we know n is odd, square-free, and $p - 1|n - 1$ for all $p|n$, we can use Chinese remainder theorem in the same manner in (a) to show that n is Carmichael. For the other way - recall the lemma on order of elements.

   Lemma 0.1. If d is the multiplicative order $a \bmod m$, i.e. the smallest positive integer d such that $a^d \equiv 1 \bmod m$, and if $a^k \equiv 1 \bmod m$ for some k, then $d|k$.

   In this case, take some $a \bmod n$ so that $a \bmod p$ is a primitive root. Then we know that $p - 1$ is the order of $a \bmod p$. Since $a^{n-1} \equiv 1 \bmod n$, thus $a^{n-1} \equiv 1 \bmod p$, so $p - 1|n - 1$.

⋆ 6. In Pohlig-Hellman, we showed two ways of calculating $k \bmod q^m$ for a prime q and integer m such that $q^m|p - 1$:
   - Directly consider q^m-th power test.
     Solution. This would be the discrete log problem with q^m possible exponents. Baby-step-Giant-step gives $O(q^{m/2+\epsilon})$ running time.
   - First calculate $k \bmod q$, then $k \bmod q^2$, ..., all the way to $k \bmod q^m$.
     Solution. The lifting process becomes the discrete log problem with q possible exponents in each step. Baby-step-Giant-step gives $O(q^{1/2+\epsilon})$ running time on each of them. Since we need to lift m times, total running time is $O(mq^{1/2+\epsilon})$.

   Compare the time complexity of these two methods for fixed q and changing m.

⋆ 7. If n is a positive integer greater than 4, The *n-th factorial* $n!$ means $n \times (n-1) \times \cdots \times 1$.

(a) If n is a composite number, show that $(n-1)! \equiv 0 \bmod n$.

Solution. Suppose n is not the square of a prime. Then we can write $n = ab$, where $1 < a < b < n$ for some a, b. Then in the product

$$(n-1)! = (n-1) \times \cdots \times b \times \cdots \times a \times \cdots \times 1$$

Thus it must be $\equiv 0 \bmod n$. If $n = p^2$ for some prime $p > 2$, then there are at least two multiples of p less than p^2. Thus $n = p^2 | (n-1)!$.

(b) If $n = p$ is a prime number, show that $(p-1)! \equiv -1 \bmod p$. This is *Wilson's theorem*.

Solution. $x^2 \equiv 1 \bmod p$ has two roots 1 or -1, so other than $1, p-1$ every number has a unique inverse (distinct from itself). Pair up every number from $2, \cdots, p-2 \bmod p$ with its inverse - this shows that the product from $2, 3, \cdots, p-2$ is actually $1 \bmod p$. Thus

$$(p-1)! \equiv 1 \cdot (2 \cdot 3 \cdot \cdots \cdot p-2) \cdot (p-1) \bmod p \equiv 1 \cdot 1 \cdot (-1) \bmod p \equiv -1 \bmod p$$

(c) Design a primality test using Wilson's theorem. What is the running time?

Solution. The naive running test is to find $(n-1)! \bmod n$ and see if it is -1 or 0. Naive algorithm involves $O(n)$ multiplication. This is bad because even the naive algorithm - the one that divides all integers up to $\sqrt{n}$, only take $O(\sqrt{n})$ operations.

Homework 8

Reference for today's lecture: Chapter 10.5 - 10.6; Chapter 11.1, Chapter 12.1-12.2

1. Recall that Euler's phi function $\phi(n)$ is the function defined by

$$\phi(n) = \text{ number of positive integers up to } n \text{ that are relatively prime to } n$$

Equivalently, $\phi(n)$ is the number of elements of $(\mathbb{Z}/n\mathbb{Z})^*$.

(a) Compute the values of $\phi(9), \phi(15), \phi(28)$.

Solution.

- $\phi(9) = 3^2 - 3 = 6$.
- $\phi(15) = \phi(3)\phi(5) = (3-1)(5-1) = 8$.
- $\phi(28) = \phi(4)\phi(7) = (2^2-2)(7-1) = 12$.

(b) If we let n have prime factorization $p_1^{e_1} \cdots p_k^{e_k}$, write down a formula for $\phi(n)$ in terms of $p_1, \cdots, p_k, e_1, \cdots, e_k$. In particular, it means that one can compute $\phi(n)$ quickly if we know the factorization of n.

Solution.

$$\phi(n) = \phi(p_1^{e_1} \cdots \phi(p_k^{e_k}) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k}) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

⋆ (c) Prove *Euler's totient function theorem*,

$$a^{\phi(n)} \equiv 1 \bmod n \text{ for all integers } a \text{ satisfying } gcd(a, n) = 1.$$

(Hint: Mimic the proof of Fermat's little theorem. Instead of looking at all the multiples of a, just look at the multiples ka with $gcd(k, n) = 1$.)

Solution. Consider the $\phi(n)$ numbers $x_1, \cdots, x_{\phi(n)} \bmod n$ that are relatively prime to n. Similar to the proof of Fermat's little theorem, the numbers $ax_1, \cdots, ax_{\phi(n)} \bmod n$ are all relatively prime to n, and are pairwise distinct - this means that these $\phi(n)$ numbers have to be a rearrangement of $x_1 \cdots, x_{\phi(n)}$!

Multiply all these $\phi(n)$ numbers, we have

$$(ax_1) \cdots (ax_{\phi(n)}) \equiv x_1 \cdots x_{\phi(n)} \bmod n \Rightarrow a^{\phi(n)}(x_1 \cdots x_{\phi(n)} \equiv x_1 \cdots x_{\phi(n)} \bmod n \Rightarrow a^{\phi(n)} \equiv 1 \bmod n$$

Cancellation of $x_1 \cdots x_{\phi(n)}$ is alright because it is relatively prime to n.

2. Using Euler's totient function theorem, or Chinese remainder theorem, or otherwise, compute

(a) $7^{26} \bmod 72$.

Solution.

$$7^{26} \equiv (-1)^{26} \bmod 8 \equiv 1 \bmod 8$$

$$7^{26} \equiv (-2)^{26} \bmod 9 \equiv 2^{26} \bmod 9 \equiv (2^3)^8 \cdot 2^2 \bmod 9 \equiv (-1)^8 \cdot 4 \bmod 9 \equiv 4 \bmod 9$$

Chinese remainder theorem gives $7^{26} \equiv 49 \bmod 72$.

(b) $3^{48} \bmod 112$.

Solution.

$$3^{48} \equiv 81^{12} \bmod 16 \equiv 1^{12} \bmod 16 \equiv 1 \bmod 16$$

$$3^{48} \equiv 27^{16} \bmod 7 \equiv (-1)^1 6 \bmod 7 \equiv 1 \bmod 7$$

Chinese remainder theorem gives $3^{48} \equiv 1 \bmod 112$.

3. Alice wishes to communicate with Bob using RSA. Suppose that Bob chooses $p = 3701$, $q = 7537$, $n = pq$ and $e = 443$.

(a) What is his private key d?

Solution. $\phi(n) = (p-1)(q-1) = 27883200$. So

$$d \equiv e^{-1} \bmod \phi(n) \equiv 10259507 \bmod 27883200$$

(b) Alice wishes to send the message $m = 11034007$. What is her ciphertext?
Solution. The ciphertext is

$$m^e \bmod n \equiv 11034007^{443} \bmod 27894437 \equiv 19717832 \bmod 27894437$$

(c) Alice sends another message, and her ciphertext is c = 3003890. What was her plaintext message?
Solution. The plaintext is

$$c^d \bmod n \equiv 3003890^{10259507} \bmod 27894437 \equiv 12990712 \bmod 27894437$$

4. A deck of 52 cards is shuffled and the top eight cards are turned over.

(a) What is the probability that the king of hearts is visible?
Solution. The king of hearts can be in any of the 52 positions. But for it to be visible when the top eight cards are turned over, it must be among the top 8. Thus the probability is $\frac{8}{52} = \frac{2}{13}$.

(b) A second deck is shuffled and its top eight cards are turned over. What is the probability that a visible card from the first deck matches a visible card from the second deck?
Solution. We count the complement - i.e. the top eight cards of the first deck and that of the second deck are distinct.
You can use any arrangement you want for the first desk. For the second one though, the first 8 cards has $52 \cdot 51 \cdot 50 \cdots 45$ possibilities. However, if you want it to be disjoint from the first 8 cards from the first deck, there are fewer possibilities.
The first card from the second deck has only 44 choices, because you can't choose any of the top 8 cards from the first desk. The second card from the second deck has only 43 choices, because you can't choose any of the top 8 cards from the first deck, and the chosen first card of the second deck. Repeating the same argument, the probability for the top eight cards of the first and second deck to be distinct is

$$\frac{44 \cdot 43 \cdot 42 \cdots 37}{52 \cdot 51 \cdot 50 \cdots 45} \sim 0.236$$

Thus the probability for some of the top eight cards of the first deck to match with that of the second deck is $1 - \frac{44 \cdot 43 \cdot 42 \cdots 37}{52 \cdot 51 \cdot 50 \cdots 45} \sim 0.764$.

5. Factorize the following numbers using Pollard's ρ method, using the polynomial $f(x) = x^2 + 1$. You can also use other polynomials, but specify them if you do so.

(a) 8051
Solution. Running Pollard's ρ method produces the following table: Here $n = 8051$.

x	y	$d = gcd(x - y, n)$
5	26	1
26	7474	1
677	871	97

Thus 97 is one of the factors. Division gives $8057 = 83 \cdot 97$.

(b) 140299
Solution. Running Pollard's ρ method produces the following table: Here $n = 140299$.

$x \bmod n$	$y \bmod n$	$d = gcd(x-y, n)$
5	26	1
26	37433	1
677	24059	1
37433	80461	1
63377	127661	1
24059	17019	1
102107	46134	1
80461	137860	1
15466	52480	1
127661	29762	1
58783	104056	1
17019	110810	1
69226	25157	1
46134	125546	1
10127	42042	1
137860	45726	1
56164	16868	307

This gives a factor 307, which is a prime. Division gives another factor 457, which is also a prime. Thus $140299 = 307 \cdot 457$.

6. Can you use RSA for key exchange? In other words, if Alice and Bob must agree on a secret key for further communication through a public channel, can they use RSA to do it?
Solution. Yes. Alice can generate a secret key and send it to Bob by RSA.

7. Eve knows that Bob is using RSA system. In particular, she knows the public key (n, e) Bob published, where $n = pq$ is a product of two large primes. Through espionage, Eve discovers $\phi(n) = (p-1)(q-1)$. How can she recover p, q and Bob's private key d?
Solution. Expanding gives $p + q = n + 1 - \phi(n)$. Since we know $p + q$ and pq in terms of n and $\phi(n)$, we can solve the quadratic equation

$$x^2 - (n + 1 - \phi(n))x + n = 0$$

to get the two roots p, q.

For the private key d, Eve only needs to compute the inverse $e^{-1} \bmod \phi(n)$.

8. Bob publishes his public key (n, e). Suppose that Eve tricks Bob into telling her his private key d. Does this help her find the factorization of n?
Solution. Yes, actually Eve can factorize n fairly easily.

By the last problem, Eve only needs to find $\phi(n)$ to factorize n. For large p, q,

$$\phi(n) = (p-1)(q-1) \asymp pq = n$$

Here $\asymp$ means "roughly of the same size" - since $p - 1$ and p are very close in value for large p.

If Eve knows the private key d, she knows that $de \equiv 1 \bmod \phi(n)$, i.e. she knows one multiple $de - 1$ of $\phi(n)$. She only needs to know which multiple $de - 1$ is. Since $\phi(n) \asymp n$, she can guess that the multiple is an integer roughly around $\frac{de-1}{n}$. Trying a few integers of that size allows her to figure out $\frac{de-1}{\phi(n)}$, thus finding $\phi(n)$, thus factorizing n.

Homework 9

Reference for today's lecture: Chapter 12.2-12.4; For $p-1$-method, see https://math.berkeley.edu/~sagrawal/su14_math55/notes_pollard.pdf

1. Compute the number of B-smooth number from 2 to X (inclusive):
   (a) $X = 25$, $B = 3$.
   Solution. 10. The numbers are $2, 3, 4, 6, 8, 9, 12, 16, 18, 24$.
   (b) $X = 35$, $B = 5$.
   Solution. 18. The numbers are $2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32$.

2. If n is B-power smooth, prove that it is also B-smooth. Is the converse true?
   Solution. If n is B-power smooth, any prime powers p^e dividing n would satisfy $p^e \leq B$. In particular, for prime factors $p = p^1$ dividing n, we have $p \leq B$, thus it is also B-smooth.
   The converse is false. For example, 4 is 2-smooth, but not 2-power smooth.

3. Use $p-1$ method to factorize
   (a) 1739.
   Solution. Let $n = 1739$. We start with base $a = 2$, $B = 11$ and keep trying to compute $gcd(a^{j!} - 1, n)$ for all $j \leq B$.

j	$x \equiv a^{j!} \bmod n$	$d = gcd(x-1, n)$
2	4	1
3	64	1
4	1083	1
5	1395	1
6	1444	37

   This shows that 37 is a factor of 1739. Division gives the factorization $1739 = 37 \cdot 47$.
   (b) 220459.
   Solution. Let $n = 220459$. We start with base $a = 2$, $B = 20$ and keep trying to compute $gcd(a^{j!} - 1, n)$ for all $j \leq B$.

j	$x \equiv a^{j!} \bmod n$	$d = gcd(x-1, n)$
2	4	1
3	64	1
4	22332	1
5	85054	1
6	4046	1
7	43103	1
8	179601	449

   This shows that 449 is a factor of 220459. Division gives the factorization $220459 = 449 \cdot 491$

4. For each of the following numbers n, compute the values of

$$n + 1^2, n + 2^2, n + 3^2, \cdots,$$

as we did in class, until you find a value $n + b^2$ that is a perfect square a^2. Then use the values of a and b to factor n.
   (a) $n = 53357$.
   Solution. $53357 + 2^2 = 231^2$. Thus $53357 = 231^2 - 2^2 = 229 \cdot 233$, both happen to be a prime.

   (b) $n = 34571$.
   Solution. $34571 + 5^2 = 186^2$. Thus $34571 = 186^2 - 5^2 = 181 \cdot 191$, both happen to be a prime.

5. Use the quadratic sieve/Dixon's method to factor the following numbers.

(a) $n = 61063$. Hint:

$$1882^2 \equiv 270 \bmod 61063 \quad \text{and} \quad 270 = 2 \cdot 3^3 \cdot 5$$
$$1898^2 \equiv 60750 \bmod 61063 \quad \text{and} \quad 60750 = 2 \cdot 3^5 \cdot 5^3$$

Solution. Multiply the two equations. Left hand side gives

$$1882^2 \cdot 1898^2 \bmod 61063 \equiv 3572036^2 \bmod 61063 \equiv 30382^2 \bmod 61063$$

Right hand side gives

$$270 \cdot 60570 \bmod 61063 \equiv (2 \cdot 3^4 \cdot 5^2)^2 \bmod 61063 \equiv 4050^2 \bmod 61063$$

Thus $30382^2 \equiv 4050^2 \bmod 61063$. Computing $gcd(30382 - 4050, 61063) = 227$, showing that 61063 has one factor being 227. Dividing shows that

$$61063 = 227 \cdot 269,$$

both happen to be a prime.

(b) $n = 52907$. Hint:

$$399^2 \equiv 480 \bmod 52907 \quad \text{and} \quad 480 = 2^5 \cdot 3 \cdot 5$$
$$763^2 \equiv 192 \bmod 52907 \quad \text{and} \quad 192 = 2^6 \cdot 3$$
$$773^2 \equiv 15552 \bmod 52907 \quad \text{and} \quad 15552 = 2^6 \cdot 3^5$$
$$976^2 \equiv 250 \bmod 52907 \quad \text{and} \quad 250 = 2 \cdot 5^3$$

Solution. Multiply the middle two equations. Left hand side gives

$$763^2 \cdot 773^2 \bmod 52907 \equiv 589799^2 \bmod 52907 \equiv 7822^2 \bmod 52097$$

Right hand side gives

$$192 \cdot 15552 \bmod 52907 \equiv (2^6 \cdot 3^3)^2 \bmod 52907 \equiv 1728^2 \bmod 52907$$

Thus $7822^2 \equiv 1728^2 \bmod 52907$. Computing $gcd(7822 - 1728, 52907) = 277$, showing that 52907 has one factor being 277. Dividing shows that

$$52907 = 277 \cdot 191,$$

both happen to be a prime.

\# 6. Prove that n is B-power smooth if and only if n divides the least common multiple of $1, 2, \cdots, B$.

Solution. Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be its prime factorization.

If n is B-power smooth, then each of these $p_1^{e_1}, \cdots, p_k^{e_k} \leq B$. Thus each of these $p_1^{e_1}, \cdots, p_k^{e_k}$ divide the least common multiple of $1, 2, \cdots, B$ (since they are among the numbers enumerated). But $p_1^{e_1}, \cdots, p_k^{e_k}$ are all relatively prime to each other, so n divides the least common multiple of $1, 2, \cdots, B$ as well.

If n divides the least common multiple of $1, 2, \cdots, B$, then $p_1^{e_1}, \cdots, p_k^{e_k}$ divides that as well. But lcm of $1, 2, \cdots, B$ being a multiple of $p_1^{e_1}$, means that at least one number $\leq B$ is already a multiple of $p_1^{e_1}$. This multiple is at most B, but is a multiple of $p_1^{e_1}$ hence at least $p_1^{e_1}$. This shows that $p_1^{e_1} \leq B$. Similarly, the other prime powers up to $p_k^{e_k} \leq B$ too.

7. Suppose Bob leaks his private key d to Eve. Instead of choosing a new n, he decides to choose a new public key e thus a new private key d, but with the same value of n. Is this safe? (That is, can Eve decrypt messages now?)

Solution. Not safe. From the last question in last problem set, we see that Eve can already factor n, thus finding $\phi(n)$. No matter how Bob chooses e, Eve can now easily compute the private key d.

8. Alice and Bob are such good friends that they choose to use RSA with the same n, but their public keys e and f are different, and indeed, they are relatively prime. Charles wants to send the same message m to Alice and Bob. If Eve intercepts both of his messages, how can she recover the plaintext message m?
Solution. Since e, f are relatively prime, Bezout's identity gives some integers u, v, such that
$$ue + vf = 1$$
Since Eve intercepted $m^e \bmod n$ and $m^f \bmod n$, she can compute
$$(m^e)^u \cdot (m^f)^v \bmod n \equiv m^{eu+fv} \bmod n \equiv m^1 \bmod n \equiv m \bmod n$$
which recovers the message.

⋆ 9. A *multiplicative function* $f : \mathbb{N} \to \mathbb{R}$ is a function such that whenever $gcd(a, b) = 1$, we have $f(a)f(b) = f(ab)$. We said in class that Euler's ϕ function is one such example.
(a) Prove that Euler's ϕ function is multiplicative.
Solution. Let $gcd(m, n) = 1$. Chinese remainder theorem says that understanding $x \bmod mn$ is equivalent to understanding $x \bmod m$ and $x \bmod n$.
Now $gcd(x, mn) = 1$ is equivalent to $gcd(x, m) = 1$ and $gcd(x, n) = 1$. This means that to find $\phi(mn)$, the number of invertible numbers mod mn, it suffices to look at all the possible pairs
(invertible numbers mod m, invertible numbers mod n)
But there are precisely $\phi(m)$ choices for the first coordinate, $\phi(n)$ choices for the second coordinate, i.e. $\phi(m)\phi(n)$ choices in total! Thus $\phi(mn) = \phi(m)\phi(n)$.
(b) The *divisor function*, $d(n)$, counts the number of divisors of n. For example, 3 has two divisors 1 and 3, so $d(3) = 2$. 12 has 6 divisors: 1,2,3,4,6,12, so $d(12) = 6$.
Prove that $d(n)$ is multiplicative.
Solution. Let $gcd(m, n) = 1$. We claim that any factor of mn is uniquely a product ab, with $a|m$ and $b|n$.
Of course, any such ab is a factor of mn. Conversely, if $d|mn$, write m, n in prime factorization. Since m, n are relatively prime, the primes in their prime factorizations are distinct. Thus any prime power factor of d must entirely divide either m, or n. Pick out the prime power factors that divide only m, and call it a. Pick out the prime power factors that divide only n, and call it b. Then $d = ab$, with $a|m$ and $b|n$. Moreover, $gcd(d, m) = a$, and $gcd(d, n) = b$. This shows the uniqueness. (Since you can rebuild a, b just by d, m and n.)
Thus, to count the number of factors of mn, it suffices to choose a factor of m, and a factor of n. There are $d(m)$ choices for factors of m, $d(n)$ choices for factors of n. Thus $d(mn) = d(m)d(n)$.
(c) Find a formula for $d(p^e)$ for a prime p and positive integer e. Deduce a formula for $d(n)$, in terms of the prime factorization of $n = p_1^{e_1} \cdots p_k^{e_k}$.
Solution. The only factors of p^e are $1, p, \cdots, p^e$. There are $e + 1$ of them, so $d(p^e) = e + 1$.
Since $d(n)$ is multiplicative, so
$$d(n) = d(p_1^{e_1} \cdots p_k^{e_k}) = d(p_1^{e_1}) \cdots d(p_k^{e_k}) = (e_1 + 1) \cdots (e_k + 1)$$
(d) The *Mobius function*, $\mu(n)$ is defined as follows.
$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by square of a prime} \\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes} \end{cases}$$
Prove that $\mu(n)$ is multiplicative.
Solution. Let $gcd(m, n) = 1$.
- If either m or n is divisible by square of a prime, so is mn. Thus
$$\mu(mn) = 0 = \mu(m)\mu(n)$$
- If both m, n are not divisible by square of a prime (i.e. square-free), let m be the product of s distinct primes, and n be the product of r distinct primes. Since $gcd(m, n) = 1$, these $r + s$ primes are all distinct as well, so mn is a product of $r + s$ distinct primes. Then,
$$\mu(mn) = (-1)^{r+s} = (-1)^s(-1)^r = \mu(m)\mu(n)$$

This proves that $\mu(n)$ is multiplicative.

⋆ 10. Here is another example of a public key cryptosystem. Bob chooses two large primes p and q and he publishes $n = pq$. It is assumed that n is hard to factor. Bob also chooses three random numbers g (where $gcd(g, n) = 1$), r_1, and r_2 modulo n and computes

$$g_1 \equiv g^{r_1(p-1)} \bmod n \text{ and } g_2 \equiv g^{r_2(q-1)} \bmod n.$$

His public key is the triple (n, g_1, g_2) and his private key is the pair of primes (p, q).

Alice wants to send the message m to Bob, where m is a number modulo n. She chooses two random integers s_1 and s_2 modulo n and computes

$$c_1 \equiv mg_1^{s_1} \bmod n \text{ and } c_2 \equiv mg_2^{s_2} \bmod n.$$

Alice then sends the ciphertext (c_1, c_2) to Bob.

Decryption is extremely fast and easy. Bob uses the Chinese remainder theorem to solve the pair of congruences

$$\begin{cases} x \equiv c_1 \bmod p \\ x \equiv c_2 \bmod q \end{cases}$$

(a) Prove that Bob's solution x equals Alice's plaintext m.

Solution. Chinese remainder theorem shows that to characterize something mod n = mod pq, it suffices to understand what they are mod p and mod q. Thus it suffices to check that $m \equiv c_1 \bmod p$ and $m \equiv c_2 \bmod q$.

Now,

$$c_1 \equiv mg_1^{s_1} \bmod n \equiv mg_1^{s_1} \bmod p \equiv mg^{r_1 s_1 (p-1)} \bmod p \equiv m(g^{p-1})^{r_1 s_1} \bmod p \equiv m \bmod p$$

Similarly, $c_2 \equiv m \bmod q$.

(b) Explain why this cryptosystem is not secure.

Solution. By Euler's totient function theorem, $g_1^{q-1} \equiv 1 \bmod n$. In particular, $ord(g_1)|q-1$. Similarly, $ord(g_2)|p-1$.

It is possible to find out the order of a particular element mod n in polynomial time. By finding the order of g_1 and g_2 and multiply them, one now has a factor d of $(p-1)(q-1)$.

Similar to the last question of Homework 7, $\phi(n) = (p-1)(q-1)$ is roughly of the same size as $n = pq$. Thus one can estimate $\phi(n)$ to be the $\frac{n}{d}$-th multiple of d. By testing the few integers around $\frac{n}{d}$, one can find $\phi(n)$, thus the factorization of n.

Homework 10

Reference for today's lecture: Chapter 11.2-11.4. Google would give you many results on hashing, signature schemes, and MACs.

1. Try to design a signature scheme based on discrete log problem. Compare your design with ElGamal signature scheme.

2. Here is another method of doing key-exchange: the Needham-Schroeder protocol.
   Suppose Alice wants to establish a shared key with Bob. They have a trusted third party Steve. K_{AS} is an established shared key between Alice and Steve, and K_{BS} is an established shared key between Bob and Steve.
   - Alice tells Steve that she wants to communicate with Bob.
   - Steve generates a symmetric key K_{AB}, to be used between Alice and Bob.
   - Steve sends Alice K_{AB}, and also $(K_{AB}, Alice)_{BS}$, the encryption of K_{AB} (and the identity of Alice) using K_{BS}.
   - Alice sends Bob $(K_{AB}, Alice)_{BS}$.

   (a) How can Bob get the shared key?
   Solution. Decrypt $(K_{AB}, Alice)_{BS}$ using the private key K_{BS}.

   (b) What can Bob do to confirm that both of them has the right shared key?
   Solution. Bob can send a random number to Alice, encrypted with K_{AB}. Ask Alice to send the random number - 1 back, encrypted with K_{AB}.

   (c) Try to attack this system.
   Solution. This is vulnerable to the replay attack. This means that Eve can use an older, compromised value of K_{AB}, and send the previously-intercepted message $(K_{AB}, Alice)_{BS}$ to Bob to start communication. This is why it is important to use a random number (called a nonce) when establishing a session key.

3. We mentioned PGP in class - there are other standards, such as GPG. Pick your favorite one and try to send an encrypted email. See https://emailselfdefense.fsf.org/en/ on how to do it.

4. Go to any website over https, and look at the certificates. Try to see how it matches up with the concepts we discussed today. You may see various modern standards being used nowadays, such as PKCS (public key cryptography standard), which would tell you the underlying cryptography method. For example, PKCS #1 is the standard published by RSA labs to tell you the format of public/private key in RSA, padding schemes, and signature scheme.

5. Random math fact: Quadratic reciprocity. Recall that Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is not a square mod } p \end{cases}$$

   The Jacobi symbol is defined similarly. For a positive integer n with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, the Jacobi symbol is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}$$

   (a) Find $\left(\frac{2}{3}\right)$, $\left(\frac{2}{5}\right)$ thus $\left(\frac{2}{15}\right)$.
   Solution. 2 is not a square mod 3, hence $\left(\frac{2}{3}\right) = -1$. 2 is not a square mod 5 either, hence $\left(\frac{2}{5}\right) = -1$. Thus,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$$

   (b) Show that if $gcd(a, n) = 1$ and a is a square mod n, then $\left(\frac{a}{n}\right) = 1$. Is the converse true?
   Solution. If a is a square mod n, then for any prime factor p of n, a is also a square mod p. Since $gcd(a, n) = 1$, we have $gcd(a, p) = 1$ as well. Hence $\left(\frac{a}{p}\right) = 1$ for any $p|n$.

If n has prime factorization $p_1^{e_1} \cdots p_k^{e_k}$, then

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k} = 1^{e_1} \cdots 1^{e_k} = 1$$

Converse is false. Part (a) is already a counterexample.

(c) The quadratic reciprocity law says that for any two primes $p, q > 2$,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

This is arguably Gauss' favorite theorem. In particular, if $q = 5$, this means that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, something you have seen in previous homework.
Compute $\left(\frac{3}{11}\right)$ with quadratic reciprocity.
Solution.

$$\left(\frac{3}{11}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{3-1}{2}}\left(\frac{11}{3}\right) = -1 \cdot \left(\frac{11}{3}\right) = -1 \cdot \left(\frac{2}{3}\right) = (-1)\cdot(-1) = 1$$

As a sanity check, we are claiming that 3 is a square mod 11. (Not contradicting part (b), since 11 is a prime) Note that indeed, $6^2 \equiv 3 \bmod 11$.

(d) Devise a way to quickly compute Jacobi symbols.
Solution. Up to a sign, one can use flip the symbol over whenever the "denominator" is larger than the "numerator". The flipping is done via quadratic reciprocity. Then the numbers can be made smaller and smaller, similar to the process of Euclidean Algorithm.

Homework 11

1. Write down a quadratic polynomial whose graph passes through $(2,4),(4,7),(8,1)$.
   Solution. Without expanding or anything, Lagrange interpolation gives
   $$4 \cdot \frac{(x-4)(x-8)}{(2-4)(2-8)} + 7 \cdot \frac{(x-2)(x-8)}{(4-2)(4-8)} + 1 \cdot \frac{(x-2)(x-4)}{(8-2)(8-4)}$$

2. Consider a card game played on a deck of 9 cards (cards 1 through 9). Alice, Bob and Eve are the players. Each player is dealt three cards.
   (a) Find an algorithm for Alice and Bob to secretly decide upon a bit (1 or 0) using only public communication, using the cards in their hand.
   Solution. See http://www.cs.umd.edu/~gasarch/COURSES/198/Su14/cards.pdf
   (b) Compare your algorithm with Diffie-Hellman. What's the difference?
   Solution. Diffie-Hellman is only secure when Eve does not have enough computational power - i.e. Diffie-Hellman is *computationally secure*. The method in part (a) however, is *information-theoretically secure*, which means that even if Eve has infinite computational power, she still cannot figure out the agreed bit.

3. Zelda has a secret to share with Alice, Bob, Carol, Donna, Edgar (yes, not Eve), Frank, and George (abbreviated A,B,C,D,E,F,G) so that
   - ABCDE can determine the secret.
   - AF can determine the secret.
   - BF can determine the secret.
   - CF can determine the secret.
   - AG can determine the secret.
   - BG can determine the secret.
   - CG can determine the secret.
   - DG can determine the secret.
   - EG can determine the secret.
   - FG can determine the secret.
   - No proper subset of the above can determine the secret.

   Can you figure out a way to do it?
   Solution. Source: http://www.cs.umd.edu/~gasarch/COURSES/198/Su14/hw08.pdf
   Use a weighted threshold scheme. Divide the secret into 21 pieces. Give A, B, C 2 pieces each, D, E 1 piece each, F 6 pieces, and G 7 pieces. For the secret to be revealed, at least 8 pieces are needed.

4. Alice solved a Sudoku puzzle just now. Bob does not believe her. Help Alice come up with a zero-knowledge proof to Bob.
   Solution. See http://www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO/

Homework 12

1. Bob also doesn't trust Eve. For some reason he has to flip a coin with Eve over phone. However, he does not know zero-knowledge proof. Can you help him design a fair coin-flipping protocol? Hint: Let $n = pq$ be product of two large distinct primes. For any squares mod n, there are 4 square roots mod n.
   Solution. See http://people.reed.edu/~jerry/361/lectures/coins.pdf, which in turn was taken from Trappe and Washington, Introduction to Cryptography.

2. We did a lot of secret sharing these two days - yet if say, Carol is mallicious, she may not use the actual given secret in the reconstruction-of-secret step. How can Zelda make sure that this does not happen? Hint: commitment schemes.
   Solution. Zelda can publish a cryptographic hash function, and publishes the hashes of each piece of the secret shared. This way every involved party can check whether a piece of secret provided by others is legitimate, by hashing it themselves.

3. Err.. you probably know what to do?

```
CICNH ITVYA EMFFG CZHJZ QLASP PMJGS GURDI FGJCC
MHQDM GKCYU MNHIT VYAEM NZITM CYFPZ HBRIM QESOJ
CILCO LAWHV YVJAA OJRGP FXWJR YHYKE EVEOF KMHXS
AFSWT JGWSC VFCTI XGUEF BTLVQ GCIAO VPMJX BLFWT
WHJZQ REOUJ DTXZH ICTMC EFLIT QVDCX YMQLF POSSL
CHMWQ EQPUC WKAGR DVFEG TDJPM GFOVY GCZSP VPPEO
PULDP MQLQW HINUE DUOEB RDRCW INGXG GERPM WQEWT
                    LFGRJ AR
```