SPCS CRYPTOGRAPHY
HOMEWORK 2

Please try all the unmarked problems. #, ⋆ problems are both optional, with ⋆ problems being harder. You are strongly encouraged to work in groups, but you have to write up the solution on your own.

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).
   (b) GCD(4, 50).
   (c) GCD(98, 35).
   (d) GCD(123, 234).
   (e) GCD(201, 335).

2. Find
   (a) The multiplicative inverse of 7 in $((\mathbb{Z}/17\mathbb{Z})^*, \times)$.
   (b) The multiplicative inverse of 7 in $((\mathbb{Z}/37\mathbb{Z})^*, \times)$.
   (c) The multiplicative inverse of 7 in $((\mathbb{Z}/101\mathbb{Z})^*, \times)$.

3. Find an integer solution to the given linear diophantine equation, or show that there are no solutions.
   (a) $7x + 17y = 1$.
   (b) $7x + 37y = 2015$.
   # (c) $7x + 37y + 59z = 2015$.
   (d) $91x + 221y = 15$.
   ⋆ (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?

4. Solve the following congruences:
   (a) $7x \equiv 1 \mod 17$.
   (b) $7x \equiv 2015 \mod 37$.
   (c) $7x \equiv 2 \mod 101$.
   (d) $x^2 \equiv 1 \mod 5$.
   (e) $x^2 \equiv 1 \mod 6$.

5. For each a in $\mathbb{Z}/7\mathbb{Z}$, determine whether there is a positive integer k such that

$$a^k \equiv 1 \mod 7$$

   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.

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

$$x^2 \equiv a \mod m.$$

   Otherwise it is called a *quadratic non-residue*.

For example, if $m = 5$, then as $1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 4 \mod 5, 4^2 = 16 \equiv 1 \mod 5$, 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.

7. (a) Suppose that $g^a \equiv 1 \mod m$, and $g^b \equiv 1 \mod m$, show that

$$g^{gcd(a,b)} \equiv 1 \mod m.$$

⋆ (b) Fix $g \mod m$. Let d be the smallest positive integer $g^d \equiv 1 \mod m$. If we also know that $g^a \equiv 1 \mod m$, prove that $d|a$.

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
```

(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`.

(b) Decrypt `YSHSSORCETIICRET`.

(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.

(d) Explain whether frequency analysis is useful for deciphering transposition ciphers.

$\star$ 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

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

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 $(5, 1)$.

(b) Explain in words, why encryption with a key $(1, k_2)$ is the same as the shift cipher with key k_2.

(c) Explain how one can decode the affine cipher given the key (k_1, k_2).

(d) If Alice and Bob send messages to each other using affine cipher, how can Eve crack the message?