HW Review: Hw's 1,2,3,4

HW 1

Vulcan Alphabet

Vulcans use an alphabet of 21 letters. They want to use an affine cipher of the form $f(x) = ax + b$. Which a can they use?

SOLUTION

The values of a they may use are

$\{1, 2, 4, 5, 6, 8, 10, 11, 13, 16, 17, 19, 20\}$

This is the set of primes in $\{1, \ldots, 21\}$ that are rel prime to 21.

NEW QUESTION:

If the alphabet was size 1147 then HOW MANY a's work?

If the alphabet was size 1000 then HOW MANY a's work?

Number of numbers rel prime to n

How many elts of $\{1, \ldots, 1146\}$ are rel prime to 1147.
Is there a name for that?

Number of numbers rel prime to n

How many elts of $\{1, \ldots, 1146\}$ are rel prime to 1147.
Is there a name for that?
$\phi(1147)$.

$\phi(p^x)$

If p is prime then $\phi(p) = p - 1$.

$\phi(p^x)$

If p is prime then $\phi(p) = p - 1$.

What about p^2?

$\phi(p^x)$

If p is prime then $\phi(p) = p - 1$.

What about p^2?
$\phi(p^2)$: Elts of $\{1, \ldots, p^2\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^2\}.$$

So there are p of them. Hence $\phi(p^2) = p^2 - p$.

$\phi(p^x)$

If p is prime then $\phi(p) = p - 1$.

What about p^2?
$\phi(p^2)$: Elts of $\{1, \ldots, p^2\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^2\}.$$

So there are p of them. Hence $\phi(p^2) = p^2 - p$.

What about p^3?

$\phi(p^x)$

If p is prime then $\phi(p) = p - 1$.

What about p^2?
$\phi(p^2)$: Elts of $\{1, \ldots, p^2\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^2\}.$$

So there are p of them. Hence $\phi(p^2) = p^2 - p$.

What about p^3?
$\phi(p^3)$: Elts of $\{1, \ldots, p^3\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^3\}.$$

So there are p^2 of them. Hence $\phi(p^3) = p^3 - p^2$.

$\phi(p^x)$

If p is prime then $\phi(p) = p - 1$.

What about p^2?
$\phi(p^2)$: Elts of $\{1, \ldots, p^2\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^2\}.$$

So there are p of them. Hence $\phi(p^2) = p^2 - p$.

What about p^3?
$\phi(p^3)$: Elts of $\{1, \ldots, p^3\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^3\}.$$

So there are p^2 of them. Hence $\phi(p^3) = p^3 - p^2$.

What about p^x?

$\phi(p^x)$

If p is prime then $\phi(p) = p - 1$.

What about p^2?
$\phi(p^2)$: Elts of $\{1, \ldots, p^2\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^2\}.$$

So there are p of them. Hence $\phi(p^2) = p^2 - p$.

What about p^3?
$\phi(p^3)$: Elts of $\{1, \ldots, p^3\}$ that are NOT rel prime to p^2:

$$\{p, 2p, 3p, \ldots, p^3\}.$$

So there are p^2 of them. Hence $\phi(p^3) = p^3 - p^2$.

What about p^x? $\phi(p^x) = p^x - p^{x-1}$.

If a, b rel prime then $\phi(ab) = \phi(a)\phi(b)$

Theorem If a, b rel prime then $\phi(ab) = \phi(a)\phi(b)$.

Proof:

A is the set of numbers in $\{1, \ldots, a\}$ rel prime to a.

B is the set of numbers in $\{1, \ldots, b\}$ rel prime to b.

C is the set of numbers in $\{1, \ldots, ab\}$ rel prime to ab.

Map $(x, y) \in A \times B$ to the z such that

$z \equiv x \pmod{a}$

$z \equiv y \pmod{b}$

$1 \leq z \leq ab - 1$. (z exists by CRT).

This map is bijection from $A \times B$ to C. So $\phi(ab) = \phi(a)\phi(b)$.

Back to our Problems

If the alphabet was size 1147 then HOW MANY a's work?

$$\phi(1147) = \phi(31 \times 37) = \phi(31)\phi(37) = 30 \times 36 = 1080$$

If the alphabet was size 1000 then HOW MANY a's work?

$$\phi(1000) = \phi(2^3 \times 5^3) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \times 100 = 400$$

We needed to factor for find $\phi(n)$.
Not know if can do much better.

KeyWord Shift and Mixed Ciphers

Alphabet is $\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o\}$.

1. A & B use *Keyword Shift Cipher* with keyword *jacob*, shift 1. Write down encoding table. Write down decoding table. Show all steps. Both table in order $a, b, c, \ldots, o$.
2. Use table to encode *FBI good, CIA bad*
3. A & B are *Keyword-Mixed Cipher* (Use $15 = 5 + 5 + 5$) with keyword *jacob*. Write down encoding table.
4. Use table to encode *FBI good, CIA bad*
5. Discuss the PROS and CONS of both the *Keyword Shift Cipher* and the *Keyword Mixed Cipher*.

Solution

a) First we write down the letters in $\{j, a, c, o, b\}$ and then the letters in $\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o\}$.
$j, a, c, o, b, d, e, f, g, h, i, k, l, m, n$
We then write this down along with the shift of 1 in this order
ENCODE:

j	a	c	o	b	d	e	f	g	h	i	k	l	m	n
a	c	o	b	d	e	f	g	h	i	k	l	m	n	j

We then put this in order:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
c	d	o	e	f	g	h	i	k	a	l	m	n	j	b

Solution Continued

DECODE: First I just swap the two rows:

c	d	o	e	f	g	h	i	k	a	l	m	n	j	b
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o

We then put this in order:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
j	o	a	b	d	e	f	g	h	n	i	k	l	m	c

Solution Continued

Actually we stop here. Some notes

1. Keyword Mixed and Keyword Shift both take a small seed and produce a quasi-random ordering of the alphabet. Playfair cipher (which I won't be going over) has the same property, though is even more random, better.
2. This was great in an earlier era when it was compared to a random perm of the 26 letters.
3. Keyword Shift a bit worse since letters towards the end of the alphabet tend to map to letters towards the end of the alphabet.

Using Vig Cipher

A and B are going to use the Vig cipher. Keyword is bill. Message:

Gradescope is okay

I used `https://www.dcode.fr/vigenere-cipher`
to obtain:

Hzlofanzqm td pslj

The spacing is the same in the input and the output. This leaks information.

Point: Software on the web may have serious problems.

Using Vig Cipher

A and B are going to use the Vig cipher. Keyword is bill. Message:

Gradescope is okay

I used `https://www.dcode.fr/vigenere-cipher`
to obtain:

Hzlofanzqm td pslj

The spacing is the same in the input and the output. This leaks information.

Point: Software on the web may have serious problems. But you knew that.

More Bad Websites

Goto the website:

`http://rumkin.com/tools/cipher/caesar.php`

Using a shift of 3 type in:

CMSC 456 Rocks! Or does it?

What does it return?

Answer:

FPVF 456 Urfnv! Ru Grhv lw?

Leaks information:

1) It leaves numbers uncoded so that 456 is 456
2) It keeps spacing.
3) It keeps caps and small letters.
4) It keeps punctuation

HW 2

Is English Program

Write a program that does the following (and run it on a sample text).
Input: A long test T.
Output: A 26-long table of DOT-PRODUCT-ING the Freq vector from T (which you got in the first program) with circular shifts $0, 1, 2, \ldots, 25$ of itself. Output alongside the dot products the amount that it was shifted by.
Note: We expect to find that shifting by 0 we get 0.065 or so and shifting by anything else we get 0.038 or so. If you do not get this then recheck your work but it may still be correct if your text T is unusual in some way.
Discuss: What did you get?

Rand Affine

In class we described the *Randomized Shift Cipher*.

Describe the *Randomized Affine Cipher* and give a small example of its use.
(Analogous to the slides with title **How to Fix without a Long Key**, and the following slide titled **Example**.

Your example should involve encoding ABAB. (Note that it should NOT map to anything of the form XYXY.)

Rand Affine

SOLUTION

Let $S = \{(a, b) \mid 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$.
The key is a function f from S to S. To send message $(m_1, \ldots, m_L)$ (each m_i a character) A does the following:

1. Pick random $r_1, \ldots, r_L \in S$.
2. For $1 \leq i \leq L$ let compute $f(r_i) = (a_i, b_i)$.
3. Send $(r_1, a_1 m_1 + b_1), \ldots, (r_L, a_L m_L + b_L)$.

To decode $(r_1, c_1), \ldots, (r_L, c_L)$ B does the following.

1. For $1 \leq i \leq L$ compute $f(r_i) = (a_i, b_i)$.
2. For each a_i find a_i^{-1}. It exists since a_i is rel prime to 26.
3. Decode as $(a_1^{-1} c_1 + b_1, \ldots, a_L^{-1} c_L + b_L)$

Example

The key is $f(a) = (3a + 1, a + 2)$ (all of the math is mod 26).
(IGNORE the fact that $3a + 1$ is not rel prime to 26 and is not a bijection.)
We want to code ABAB which is 0101.
Need four ordered pairs.

Rand 2, maps to (7,4), so 0 maps to $7 * 0 + 4 = 4 = e$
Rand 3, maps to (10,5), so 1 maps to $10 * 1 + 5 = 15 = o$
Rand 10, maps to (5,12), so 0 maps to $5 * 0 + 12 = 12 = m$
Rand 15, maps to (20,17), so 1 maps to $15 * 1 + 17 = 32 \equiv 6 = g$

So A sends eomg.

How would Eve Attack Rand Affine?

Eve gets to see the r's.
If she see's enough messages she will see the same r many times.
Do Freq analysis on that.
Leave it to you to formalize this.

Rand X

Can define Randomized 2×2–Matrix, Randomized-Vig, etc.
Leave this to you to do.
Leave this to you to see how to crack.

1-time Pad

A and B are going to use the 1-time pad. They will meet and generate randomly a 999,999,999-bit key. The first message A wants to send to B is 110011. What is the probability that A sends 000000? How about 110011? How about 111000?

SOLUTION

The prob that the first message is 110011 is the prob that the key is a particular 6-bit string. Since the key is uniformly random, that prob is $\frac{1}{2^6}$. Same for all of the 6-bit strings given above.

Inverses Mod 15

1. Which numbers in $\{1, 2, 3, \ldots, 14\}$ have an inverse mod 15?
2. For all such numbers, give the inverse.

Solution

Thought Process: look at numbers that are $\equiv 1 \pmod{15}$

$$1, 16, 31, 46, 61, 76, 91, 106, 121$$

Given x I want y such that

$$xy \in \{1, 16, 31, 46, 61, 76, 91, 106, 121\}$$

Skip numbers NOT rel prime to 15, they won't have inverses.
1 has inverse 1
2 divides 16. Great: $2 \times 8 = 16 \equiv 1$
4 divides 16. Great! $4 \times 4 = 16 \equiv 1$
7 divides 91. Great! $7 \times 13 = 91 \equiv 1$
8 Already have $2 \times 8 \equiv 1$
11 divides 121. Great: $11 \times 11 \equiv 1$
13 Already have $7 \times 13 \equiv 1$
14 Gee, only number left is 14. $14 \times 14 \equiv 1$

HW 3

Repeated Squaring Method

Do the following using the repeated squaring method. Show your work.

1. $14^{26} \pmod{1000}$
2. $30^{14} \pmod{1000}$

SOLUTION All $\equiv$ are mod 1000

$14^{2^0} \equiv 14$
$14^{2^1} \equiv ((14^{2^0})^2 \equiv 196$
$14^{2^2} \equiv ((14^{2^1})^2 \equiv 196^2 \equiv 38416 \equiv 416$
$14^{2^3} \equiv ((14^{2^2})^2 \equiv 416^2 \equiv 173056 \equiv 56$
$14^{2^4} \equiv ((14^{2^3})^2 \equiv 56^2 \equiv 3136 \equiv 136$
Write 26 as sum of powers of 2: $26 = 2^4 + 2^3 + 2^1$. Hence:
Note: After doing the 14^{2^i}'s still need to do some stuff.

$$14^{30} \equiv 14^{2^4} \times 14^{2^3} \times 14^{2^1}$$

$$\equiv (136 \times 56) \times 196 \equiv 7616 \times 196 \equiv 616 \times 196 \equiv 120736 \equiv 736.$$

Diffie-Helman for Three

$14^{2^0} \equiv 14$

Modify Diffie-Helman key exchange so that three people share a secret.

State carefully exactly what function Eve needs to compute to find the shared secret, with which inputs.

Diffie-Helman for A,B,C

1. A randomly obtains a prime p and a generator $g \in \{2, \ldots, p-1\}$
2. A makes (p, g) public (so B, C and Eve all see it).
3. A picks a at random and sends g^a to everyone
4. B picks b at random and sends g^b to everyone
5. C picks c at random and sends g^c to everyone.

Not Done Yet.

Diffie-Helman for A,B,C

Recap:
Alice has private a, Bob has private b, Carol has private c.
g^a, g^b, g^c are public.

1. A computes $(g^b)^a = g^{ab}$ and sends it to everyone.
2. B computes $(g^c)^a = g^{ac}$ and sends it to everyone.
3. C computes $(g^b)^c = g^{bc}$ and sends it to everyone.
4. A computes $(g^{bc})^a = g^{abc}$ which is the secret!
5. B computes $(g^{ac})^b = g^{abc}$ which is the secret!
6. C computes $(g^{ab})^c = g^{abc}$ which is the secret!

Hardness Assumption

Eve has to be able to compute following function.
INPUT: $p, g, g^a, g^b, g^c, g^{ab}, g^{ac}, g^{bc}$
OUTPUT: g^{abc}.
Hardness Assumption: That function is hard to compute.

Programs to find Safe Primes and Generators

1. POWER: Given g, p, n compute, $g^n \pmod{p}$.
2. TESTPRIME: Given p test if prime. Use not-quite-correct method.
3. TESTSAFEPRIMES: Given p test if p is a SAFE prime. Use program to find first 10 safe primes ≥ 1000. Call them $p_1, \ldots, p_{10}$.
4. Given a Safe prime p and a number $g \in \{1, \ldots, p-1\}$ test if g is a generator. Use the program to find, for each p_i from the last problem, the smallest generator mod p_i.
5. Get Data: Are $\sim \frac{1}{2}$ of $\{1, \ldots, p-1\}$ generators?

SOLUTION

POWER: $g^n \pmod p$. Use repeated squaring

TESTPRIME: pick $lg(p)$ random a and test if $a^p \equiv a \pmod p$.
If any NO then NOT PRIME.
If all YES then output YES PRIME, but could be wrong (low probability)

TESTSAFEPRIMES: TESTPRIME(p) AND TESTPRIME($\frac{p-1}{2}$)
Given a Safe prime p and a number $g \in \{1, \ldots, p-1\}$ test if g is a generator. Computer $g^{(p-1)/2} \pmod p$. If $\equiv 1$ NOT Gen, if $\not\equiv 1$ IS gen. Fun Fact: Will always be 1 or -1.

Get Data: Are $\sim \frac{1}{2}$ of $\{1, \ldots, p-1\}$ generators?
Discuss What did you find?

SOLUTION

1. Write psuedocode that will create a random number with ROUGHLY n bits (could be off by a constant) of the form $30k + 1$.
2. Discuss PROS and CONS of picking random primes in this manner.

SOLUTION

a) The idea is to pick a random k of length m (we determine m later) and then look at $30k+1$. So we need m so that $30k+1$ is n bits. 30 is approximately 32. Hence $32k$ is around $m+5$ long. Hence we pick $m = n-5$.

1. Input n
2. Pick a random $m-6$ bit string k'.
3. Let $k = 1k'$ (in binary).
4. Output $30k+1$.

b) PRO- Find prime faster since candidates not div by 2,3, or 5. How much faster? There are 2^n n-bit numbers. Hence the search space is usually 2^n. Now the search space is only $\frac{2^n}{30}$.
CON- A clever Number Theorist may be able to use that your prime is $\equiv 1 \pmod{30}$.

Diffie-Helman Question

I asked for you to carry out Diffie-Helman. I won't go over that here but I want to talk about the last two parts.

1. What is the secret written in binary? Use 8 bits since $2^7 < 107 < 2^8$. There can be leading 0's.
2. Why might A and B use the answer in binary?

SOLUTION

The secret is 12 which in binary is 00001100
A and B end up with a fairly random sequence of 0's and 1's.
They can use this for a 1-time pad.

Question: Is the sequence they get Random? Psuedorandom (we have not defined that formally yet)? Discuss

HW 4

$a^N \pmod p$ where N is Ginormous

1. Give an algorithm (psuedocode) to compute $a^n \pmod p$ efficiently even if n is ginormous – say $n \geq 10^{10^{10^{p!}}}$!, and p is a prime. (HINT: Repeated Squaring may be part of the answer but is not, by itself, enough.)
2. Use your method to compute, by hand, $14^{999,999,999} \pmod{107}$. (You can use a calculator but show all steps.)
3. Discuss how to compute $a^n \pmod p$ efficiently if n is ginormous- say $n \geq 10^{10^{10^{p!}}}$!, and p is A COMPOSITE. There IS a bottleneck to doing this – what is it? Why was it NOT a problem when p is prime?

SOLUTION

a) Recall that $a^n \pmod p \equiv a^{n \pmod{p-1}} \pmod p$.

1. Input(a, n, p)
2. Divide n by $p-1$ and let n' be the remainder. NOTE: $0 \leq n' \leq p-2$, so n' is SMALL
3. Compute $a^{n'} \pmod p$ using repeated squaring.

SOLUTION

b) When you divide 999,999,999 by 107 you get remainder 41.
So we now do $14^{41} \pmod{107}$.
$14^{2^0} \equiv 14$
$14^{2^1} \equiv ((14^{2^0})^2 \equiv 196 \equiv 89$
$14^{2^2} \equiv ((14^{2^1})^2 \equiv 89^2 \equiv 7921 \equiv 3$
$14^{2^3} \equiv ((14^{2^2})^2 \equiv 3^2 \equiv 9$
$14^{2^4} \equiv ((14^{2^3})^2 \equiv 9^2 \equiv 81$
$14^{2^5} \equiv ((14^{2^4})^2 \equiv 81^2 \equiv 34$
We write 46 as a sum of powers of 2: $41 = 2^5 + 2^3 + 2^0$.
Hence

$$14^{41} \equiv 14^{2^5} \times 14^{2^3} \times 14^{2^0} \equiv 34 \times (9 \times 14 \equiv)$$

$$34 \times 126 \equiv 34 \times 19 \equiv 646 \equiv 4$$

SOLUTION

c) We can use that $a^n \pmod{p} \equiv a^{n \pmod{\phi(p)}} \pmod{p}$.
PRO- $n \mod \phi(p)$ will be smaller than p, so small.
CON- computing $\phi(p)$ might be hard. For p prime it was easy.
If p is composite $\phi(p)$ can be done with factoring. But Factoring is prob hard. There may be another way, but it won't be discovered until Aaron gets his PhD in Number Theory.

RSA Problem

1. A and B are going to do RSA with $p = 11$ and $q = 13$,
2. What is the value of N?
3. What is the value of R
4. What is the least $e \geq \frac{R}{6}$ that A can use?
5. For that e, find the correct d. (you can use a program you find on the web but you must tell us what it is.)
6. B wants to send the message 10. What does he send? (Use repeated squaring and show all step.)

RSA Problem– SOLUTION

a) $N = pq = 11 \times 13 = 143$
b) $R = (p-1)(q-1) = 10 \times 12 = 120$
c) $R/6$ is 20. We need to pick the least $e \geq 20$ such that e is rel prime to 120. $e = 23$ works.
d) Need d such that $ed \equiv 1 \pmod{120}$.
I used the program at `https://planetcalc.com/3311/`
The answer was 47.

RSA Problem– SOLUTION

e) To send 10 B must send
$10^{23} \pmod{143}$. We omit the solution.
$10^{2^0} \equiv 10$
$10^{2^1} \equiv 100$
$10^{2^2} \equiv 100 \times 100 \equiv (-43)(-43) \equiv 1849 \equiv 133$
$10^{2^3} \equiv 133 \times 133 \equiv (-10)(-10) \equiv 100$
$10^{2^4} \equiv 100 \times 100 \equiv 133$
So
$10^{23} \equiv 10^{16} \times 10^4 \times 10^2 \times 10^1 \times 10^0 \equiv 133 \times 133 \times 100 \times 10 \times$

$$\equiv 133 \times 133 \times 100 \times 10 \times \equiv (-10)(-10)(100)(10) \equiv$$

$$(100)(100)(10) \equiv 133 \times 10 \equiv -10 \times 10 \equiv -100 \equiv 33.$$

Another RSA Problem

A and B are going to do RSA with $p = 17$ and $q = 19$,

1. What is the value of N?
2. What is the value of R
3. If A uses $e = 2$ then for which m is Eve EASILY able to decode the message?
4. If B wants to send $m = 3$ then for which e is Eve EASILY able to decode the message?

Another RSA Problem–Solution

1) $N = pq = 17 * 19 = 323$
2) $R = (p-1)(q-1) = 288$
3) $e = 2$ BAD choice: 2 not rel prime to 288. (my bad)
$e = 2$ BAD choice: sqrt has non unique answer. (my bad)
Two BAD's related: Need e rel prime to R so answer unique.
More General: e not rel prime to R then can't decode uniquely.

Back to the problem:
To send m, B sends $m^e \pmod N$ so $m^2 \pmod{323}$.
For m small $m^2 \pmod{323}$ will be ordinary m^2. Eve can take a normal square root and get the answer.
If $m^2 < 323$, sqrt is easy. That occurs when $m \leq 17$.

Another RSA Problem–Solution

4) If B wants to send m then he sends $m^e \pmod{N}$ so $3^e \pmod{323}$.

For e small it will $3^e \pmod{323}$ will be the ordinary 3^e, and then Eve can take a log base 3 (easy in the normal numbers, hard in mod 323) and get the answer.

So long as $3^e < 323$, it will be easy to determine m. That occurs when $m \leq 5$.

Key Exchange Variant-SET UP

Suppose that Professor Cowz has a key-exchange protocol P with the following properties. There is a security parameter n.

1. If A and B use the protocol to share a message of length n (meaning the message is n binary bits long) then the following occurs:
   - If Eve cracks it, she can use that to factor numbers of length n. (Hence we think that for n large enough Eve cannot crack it.)
   - Before the protocol Eve is looking at 2^n possible shared secret keys it could be. If she was to try to figure out which one, she would have a $\frac{1}{2^n}$ chance of getting it right. We will assume that AFTER the protocol she STILL has only a $\frac{1}{2^n}$ chance of getting it right (unless she can factor).
   - At the end of the protocol A and B share a message s of length n. They did NOT get to control the message.

Key Exchange Variant-QUESTIONS

QUESTIONS:

1. (10 points) (Look up on the web for this one and cite your source.) Complete this sentence: If $n \geq XXX$ then Eve will not be able to find the shares secret key.
2. (20 points) Show how A and B can use Cowz's key-exchange protocol to create a public key cryptosystem (where they can send what they want). Its OKAY if it has a small bias in it.

Key Exchange Variant-ANSWERS

1) According to `http://mathworld.wolfram.com/RSANumber.html` The RSA challenge has challenged people to factor larger and larger numbers. The current winners is 232 DECIMAL digits so around 700 bits. We'll make it an even 1000 bits just to be sure.

2) A wants to send B m of length n. They first do the key-exchange protocol. They both now have a string s of length n. Eve has NO IDEA what s is. A then sends B $m \oplus s$.