Cryptography & Encryption:6G7Z1011

Keith Yates

January 25, 2019

Cryptography & Encryption:6G7Z1011 : Simple Ciphers , Statistical Analysis and $\mathbb{Z}(n)$

Keith Yates

January 25, 2019

Caesar

Recall from last week, we meet the Caesar cipher, it worked by using a key which 'pushed on' each letter by a fixed amount. So if key $K = 3$ then A mapped to A $+3$ = D, and so on.

Permutation Cipher

We now consider the *permutation cipher*, a permutation is (recalling notation from the last lecture) a bijection from the alphabet to itself, in plainer terms it jumbles the letters up.

plain	a	b	c	d	e	f	...
cipher	z	p	n	e	a	g	...

so 'cab' becomes 'nzp'.
The Caesar cipher had 26 possible keys, whilst the permutation cipher has $26! = 26 \times 25 \times 24$ keys; however it is no more secure than the Caesar cipher, why?

Statistical analysis

Both the Caesar cipher, the affine cipher and the permutation cipher suffer from the same major flaw, they are amenable to attack by statistical analysis.

Attacking the permutation cipher

The permutation cipher has 26! keys, so how long would a brute force attack take to do. Say you had a computer that could test 10^9 keys per second (clock speed of a chip is $\approx 10^9$) then to 'crack' the code would take

$$\frac{26!}{10^9} \approx 16! \text{ seconds} \tag{0.1}$$

Statistical attack

The flaw in the ciphers discussed to date is they always encode a letter in the same way, as such if you read an encrypted message and keep a count of how many times each character appears then the letter with the most counts will be one of the vowels, and the letters with the fewest counts will tend to be 'z'.
A lab question asks you to confirm this.

Affine Cipher

We now look at the affine cipher, it suffers the same problem as the Caesar and the permutation cipher but it uses techniques that are required in 'real world' ciphers.
We need some mathematics

Introducing $\mathbb{Z}(n)$

We define

$$\mathbb{Z}(n) = \{0, 1, 2, \ldots n-1\}\,. \tag{0.2}$$

And we define addition $+$ and multiplication $\times$ in the usual manner except we remove any multiples of n. For example, in $\mathbb{Z}(7)$ then

$$4 \times 3 =_{\mathbb{Z}(7)} 5. \tag{0.3}$$

because in $\mathbb{Z}$

$$4 \times 3 =_{\mathbb{Z}} 12 =_{\mathbb{Z}} (7)^{\text{remove}} + 5 \tag{0.4}$$

From now on I will omit the subscript in $=_{\mathbb{Z}(n)}$ and just write $=$, If I want to emphasise which system I am working in I may write

$$4 \times 3 = 5 \mod 7. \tag{0.5}$$

Simple Problem in $\mathbb{Z}(6)$

A simple problem, please evaluate the cells $(\mathbb{Z}(6), \times)$. I have done some, for example

$$2 \times 4 = 6 + 2, \quad \text{so } 2 \times 4 = 2 \mod 6. \tag{0.6}$$

	0	1	2	3	4	5
0						
1						
2				0	2	
3						
4						
5						

Table: $\mathbb{Z}(6)$

Simple Problem in $\mathbb{Z}(5)$

A simple problem, please evaluate the cells $(\mathbb{Z}(5), \times)$.

	0	1	2	3	4
0					
1					
2					
3					
4					

Table: $\mathbb{Z}(5)$

Coding

The above two examples are interesting from an encryption view point. Suppose we proposed an encryption algorithm that was just multiplication $\mod n$. Then we are in difficulties because we have lost injectivity in the $n = 6$ case, the $n = 5$ case does work.
Important point: our coding techniques require the n in $\mathbb{Z}(n)$ to have rather special properties.

Affine Cipher

The affine cipher is defined for a key $(a, b) \in \mathbb{Z}(26)$ by

$$\phi : \mathbb{Z}(26) \to \mathbb{Z}(26), \quad x \mapsto e(x) = ax + b \mod 26 \tag{0.7}$$

where x is the 'plain' integer and $ax + b$ is its encryption. For example, if $(a, b) = (3, 5)$ and $x = 6$ then it encrypts

$$6 \mapsto 3 \times 6 + 5 = 23. \tag{0.8}$$

Note if $a = 1$ then the affine Cipher reduces to the Caesar cipher.

Affine Cipher

The affine Cipher is interesting from a learning viewpoint, suppose I pick $(a, b) = (4, 7)$

$$\phi : \mathbb{Z}(26) \to \mathbb{Z}(26), \quad x \mapsto e(x) = 4x + 7 \mod 26 \tag{0.9}$$

Note

1. $x = 1$ then $e(x) = 4 \times 1 + 7 = 11 \mod 26$, and
2. $x = 14$ then

$$e(x) = (4{\times}14){+}7 = 56{+}7 = 63 = (26{\times}2){+}11 \mod 26. \tag{0.10}$$

Disaster, the function is no longer injective. In cryptographic terms $(4, 7)$ is NOT a valid key.

Determining the valid keys for the affine cipher

What are the valid keys for the affine cipher? Or, for what values of $a, b \in \mathbb{Z}(26)$ does

$$ax_1 + b = ax_2 + b \mod 26 \tag{0.11}$$

imply $x_1 = x_2$?

prime and relatively prime

Recall

1. The *greatest common denominator* of two numbers a and b is the larger integer that divides both a and b, and we write this $\gcd(a, b)$.
2. A number is termed *prime* if its only divisors are one and itself.
3. Two numbers are termed *relatively prime* if their largest common divisor is 1

For example 11 is prime; the numbers 15 and 22 are relatively prime (though neither is prime).

composite, pseudoprime , Carmichael

Let $n \in \mathbb{N}$ ($\mathbb{N} = \{1, 2, 3, \ldots\}$).

1. n is termed *composite* if $n > 1$ and n has a divisor.
2. n is termed *pseudoprime* to the base a if n is odd, composite and $a^{n-1} \equiv 1 \mod n$.
3. If n is pseudoprime to the base a for all integers a with $\gcd(a, n) = 1$ then n is termed a *Carmichael* number.

Carmichael numbers

Show that 561 is a Carmichael number.

Code

We have $561 = 3.11.17$, and the number is clearly odd and composite. We need to form the set

$$A = \{i \in \mathbb{N} \mid \gcd(i, 561) = 1\} \tag{0.12}$$

and for each $a \in A$ we need to check

$$a^{561-1} \equiv 1 \mod n \tag{0.13}$$

This is rote coding problem (that requires a for loop).

solutions to equations mod 26

Recall we wish the affine function to be injective. That is for any $y \in \mathbb{Z}(26)$ then

$$ax + b = y \mod 26 \tag{0.14}$$

has a unique solution for x. Writing this

$$ax = y - b \mod 26. \tag{0.15}$$

As y runs over all of $\mathbb{Z}(26)$ so does $y - b$ (recall b is fixed), so the question becomes: for what values of a does

$$ax = y \mod 26. \tag{0.16}$$

have a unique x solution for each $y \in \mathbb{Z}(26)$?

Key space sizes

Determining the key space

Caesar cipher	26
Permutation cipher	26!
Affine Cipher	?

Table: The key space is the number of keys available to an encryption algorithm, and for obvious reasons an encryption algorithm needs a large key space.

Solution

The equation

$$ax = y \mod 26. \tag{0.17}$$

has a unique solution in x for each $y \in \mathbb{Z}(26)$ if and only if $\gcd(a, 26) = 1$

Proof.

- $\Rightarrow$: Suppose $\gcd(a, b) = d > 1$ then picking (for example) $y = 0$ then we need to solve $ax = 0 \mod 26$, and we have at least two solutions: $x = 0$ and $x = \frac{26}{d}$.

$\Leftarrow$

Proof.

- $\Leftarrow$: Let $\gcd(a, 26) = 1$ and (arguing to the contrary) suppose there are two solutions

$$ax_1 = y \mod 26 \quad \text{and} \quad ax_2 = y \mod 26 \tag{0.18}$$

then

$$a(x_1 - x_2) = 0 \mod 26. \tag{0.19}$$

So $a(x_1 - x_2)$ is a multiple of 26, or turning this around $26 \mid a(x_1 - x_2)$. However $\gcd(a, 26) = 1$ so $26 \mid x_1 - x_2$ thus $x_1 = x_2 \mod 26$.

Euler ϕ Function

The *Euler* ϕ function is defined

$$\phi : \mathbb{N} \to \mathbb{N}, \quad n \mapsto |\{i \in \mathbb{N} \mid 1 \leq i \leq n, \gcd(n, i) = 1\}.| \tag{0.20}$$

In English, for each $n \in \mathbb{N}$ the $\phi(n)$ is the number of integers less than or equal to n that are relatively prime to n.

Euler's function

Evaluate the Euler ϕ function in the range $1 \leq i \leq 10$.

i	$\phi(i)$
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Table: Euler

Solution

i	$\phi(i)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

Table: Euler's totient

Some working out, $\phi(9)$

1	2	3	4	5	6	7	8	9
✓	✓	✗	✓	✓	✗	✓	✓	✗

Table: What is $\phi(9)$, a tick indicates $\gcd(i, 9) = 1$

$\phi(9) = 6$, count the ticks.

Some working out, $\phi(10)$

1	2	3	4	5	6	7	8	9	10
✓	✗	✓	✗	✗	✗	✓	✗	✓	✗

Table: What is $\phi(10)$, a tick indicates $\gcd(i, 10) = 1$

$\phi(10) = 4$, count the ticks.

key space for the affine cipher

Recall, we are still trying to evaluate the key space for the affine cipher. Now note that every integer has an unique (to within the order) multiplicative decomposition has a product of primes, for example

$$100 = 2^2 5^2. \tag{0.21}$$