Scribe: Cryptography and Network Security (Class 3)

Smayan Das

4-Sep-2020

1 Introduction

Substitution ciphers encrypt the plaintext by swapping each letter or symbol in the plain text by a different symbol as directed by the key.
The Affine Cipher is a type of mono-alphabetic substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. As such, it has the weaknesses of all substitution ciphers.

2 The Affine Cipher

In the Affine Cipher the letters of an alphabet of size m are first mapped to the integers in the range [0,m-1] = Z_m. It then uses modular arithmetic to transform the integer that each plaintext letter corresponds to into another integer that correspond to a ciphertext letter.

2.1 Encryption

The encryption key for an affine cipher is an ordered pair of integers, both of which come from the set [0,m-1], where m is the size of the character set being used (for us, the character set is the English alphabet, so we have m = 26). So, the first step in the encryption process is to transform each of the letters in the plaintext alphabet to the corresponding integer in the range 0 to m-1. With this done, the encryption process for each letter is given by

$$E(x) = (ax + b) \bmod m$$

where a and b are the key for the cipher. This means that we multiply our integer value for the plaintext letter by a, and then add b to the result. Finally, we take this modulus m.

One thing to note is that the value a must be chosen such that a and m are co-prime otherwise the encrypted cipher cannot be decrypted, the reason for which will be explained later. This essentially means that some of the possible pairs of integers from the set [0,m-1] = Z_m are not valid as affine encryption keys.

The mapping between plaintext alphabet and plaintext value is as given below:

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

As an example, the encryption of the plaintext "affine cipher", using the keys a = 5, b = 8 is given below. Note that here, a = 5 is a valid affine encryption cipher as 5 is co-prime to m = 26.

Plaintext	a	f	f	i	n	e		c	i	p	h	e	r
x	0	5	5	8	13	4		2	8	15	7	4	17
5x+8	8	33	33	48	73	28		18	48	83	43	28	93
(5x+8) mod 26	8	7	7	22	21	2		18	22	5	17	2	15
Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P

2.2 Modular Multiplicative Inverse

Before moving forward with the decryption part it is important to know about Modular Multiplicative Inverse. A modular multiplicative inverse of an integer a is an integer x such that the product ax is congruent to 1 with respect to the modulus m. In the standard notation of modular arithmetic this congruence is written as

$$ax \equiv 1 \bmod m$$

which is the shorthand way of writing the statement that m divides (evenly) the quantity ax-1, or, put another way, the remainder after dividing ax by the integer m is 1. This also means that, $a^{-1} = x$ and $x^{-1} = a$ w.r.t modulo m. The value of x should be in 1, 2, ... m-1 or Z_m^*, i.e., in the range of integer modulo m.

The multiplicative inverse of "a modulo m" exists if and only if a and m are relatively prime (i.e., if $gcd(a, m) = 1$).This can easily be proved as shown below:

Proof. Let's assume by contradiction that $gcd(a, m) > 1$ and e is the inverse of a w.r.t modulo m. Then we can say that $m|(ae-1)$. Now as $k|m$ then $k|(ae-1)$. Also, $k|e$ then $k|ae$ This in turn implied that $k|1$ which is not possible. This implies that k—1 which is a contradiction and hence the proof is complete. □

Another interesting property is that if m is a prime number, p then every element has an inverse. Then Z_p is called a field.

2.3 Decryption

In deciphering the ciphertext, it is required to perform the opposite (or inverse) functions on the ciphertext to retrieve the plaintext. Once again, the first step is to convert each of the ciphertext letters into their integer values. This is done as follows:

$$D(x) = a^{-1}(x - b) \bmod m$$

where a^{-1} is the modular multiplicative inverse of a modulo m, i.e. it satisfies the equation:

$$aa^{-1} \equiv 1 \bmod m$$

The modular multiplicative inverse of a w.r.t m exists only if a and m are co-prime. This is why it was important to select the affine encryption key, a which was co-prime to m. The possible values of a such that $gcd(a, 26) = 1$ are:

$$1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$$

The decryption of the encryption for the text "affine cipher" is shown below:

Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P
y	8	7	7	22	21	2		18	22	5	17	2	15
21(y - 8)	0	-21	-21	294	273	-126		210	294	-63	189	-126	147
21(y - 8) mod 26	0	5	5	8	13	4		2	8	15	7	4	17
Plaintext	a	f	f	i	n	e		c	i	p	h	e	r

It can be shown as follows that decryption function is the inverse of the encryption function,

$$\begin{aligned} \mathrm{D}(\mathrm{E}(x)) &= a^{-1}(\mathrm{E}(x) - b) \bmod m \\ &= a^{-1}(((ax + b) \bmod m) - b) \bmod m \\ &= a^{-1}(ax + b - b) \bmod m \\ &= a^{-1}ax \bmod m \\ &= x \bmod m. \end{aligned}$$

2.4 Key Size of Affine Cipher

The possible values of a such that $gcd(a, 26) = 1$ are:

$$1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$$

and b can be any one of 26 possibilities. So total key size is $12 * 26 = 312$ As is evident the key size is too small. A generalized form of the key size can be derived using Euler's Totient function for any m.

3 Euler's Totient Function

The number of positive integers in $Z_m (m > 1)$, that are relatively prime to m and does not exceed m is denoted by $\Phi(m)$, called Euler's Totient function or phi function.

3.1 Multiplicative Property

For any two integers $m, n > 1$ if $gcd(m, n) = 1$ then:

$$\Phi(mn) = \Phi(m) * \Phi(n)$$

Proof. To prove this, we make a rectangular table of the numbers 1 to mn with m rows and n columns, as follows:

1	m+1	2m+1	.	.	(n-1)m+1
2	m+2	2m+2	.	.	(n-1)m+2
3	m+3	2m+3	.	.	(n-1)m+3
.	.	.	.	.	.
.	.	.	.	.	.
m	2m	3m	.	.	nm

The numbers in the r^{th} row of this table are of the form km + r as k runs from 0 to $m - 1$.
Let $d = gcd(r, m)$. If $d > 1$ then no number in the r^{th} row of the table is relatively prime to mn, since $d|(km + r)$ for all k. So to count the residues relatively prime to mn we need only to look at the rows indexed by values of r such that $gcd(r, m) = 1$, and there are $\Phi(m)$ such rows.
If $gcd(r, m) = 1$ then every entry in the r^{th} row is relatively prime to m, since $gcd(km + r, m) = 1$ by the Euclidean algorithm. The entries in such a row form a complete residue system modulo n. Thus, exactly $\Phi(n)$ of them will be relatively prime to n, and thus relatively prime to mn.
We have shown that there are $\Phi(m)$ rows in the table which contain numbers relatively prime to mn, and each of those contain exactly $\Phi(n)$ such numbers. So there are, in total, $\Phi(m) * \Phi(n)$ numbers in the table which are relatively prime to mn. This proves the theorem. □

3.2 Value for power of a prime

If p is prime and $k \geq 1$, then

$$\varphi\left(p^k\right) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

Proof. Since p is a prime number the only possible values of $gcd(p^k, m)$ are $1, p, p^2, ..., p^k$, and the only way for $gcd(p^k, m)$ to not be equal to 1 is for m to be a multiple of p. The multiples of p that are less than or equal to p^k are $p, 2p, 3p, ..., p^{k-1}p = p^k$, and there are p^{k-1} of them.
Therefore, the other p^k - p^{k-1} numbers are all relatively prime to p^k. □

3.3 Euler's product formula

It states

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is over the distinct prime numbers dividing n.

Proof. The fundamental theorem of arithmetic states that if $n > 1$ there is a unique expression for n,

$$n = {p_1}^{k_1} \cdots {p_r}^{k_r},$$

where $p_1 < p_2 < ... < p_r$ are prime numbers and each $k_i \geq 1$.(The case n=1 corresponds to the empty product.) Repeatedly using the multiplicative property of Φ and the formula for $\Phi(p^k)$ gives:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r}) \\
&= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

□

4 Conclusion

Hence for a particular character set of size m the maximum number of affine encryption keys possible is $m * \Phi(m)$. If m is a prime then $\Phi(m) = m$-1. So for prime m, the number of affine encryption keys possible is $m * (m - 1)$

5 References

- https://en.wikipedia.org/wiki/Affine_cipher
- https://crypto.interactive-maths.com/affine-cipher.html
- http://practicalcryptography.com/ciphers/affine-cipher/
- https://math.asu.edu/sites/default/files/affine.pdf
- http://stanford.edu/~dntse/classes/cs70_fall09/cs70_fall09_5.pdf

- https://en.wikipedia.org/wiki/Modular_multiplicative_inverse
- https://en.wikipedia.org/wiki/Euler%27s_totient_function