Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 26, 2020, No. 4, 213–222
DOI: 10.7546/nntdm.2020.26.4.213-222

Significant role of the specific prime number $p = 257$ in the improvement of cryptosystems

Hana Ali-Pacha [1], Naima Hadj-Said [2], Adda Ali-Pacha [3] and Özen Özer [4,*]

[1] Laboratory of Coding and Security of Information,
University of Sciences and Technology of Oran
USTO, 1505 El M'Naouer Oran 31000 Algeria
e-mail: hana.alipacha@univ-usto.dz

[2] Laboratory of Coding and Security of Information,
University of Sciences and Technology of Oran
USTO, 1505 El M'Naouer Oran 31000 Algeria
e-mail: naima.hadjsaid@univ-usto.dz

[3] Laboratory of Coding and Security of Information,
University of Sciences and Technology of Oran
USTO, 1505 El M'Naouer Oran 31000 Algeria
e-mail: a.alipacha@gmail.com

[4] Department of Mathematics, Faculty of Science and Arts,
Kırklareli University
Kirklareli, 39100, Turkey
e-mail: ozenozer39@gmail.com

* *Corresponding author*

Received: 15 January 2020 **Revised:** 22 September 2020 **Accepted:** 15 November 2020

Abstract: Cryptology is the significant science which is inseparable from the means of communication of secrets. In a safe manner, it has the main objective of transmitting (potentially sensitive) information between two interlocutors. One distinguishes mainly two "dual" disciplines within cryptology:

(a) cryptography, which is interested in the security of information.

(b) cryptanalysis, which seeks to attack it.

One have a starting set of 256 elements, we add a new element to this set to form a set of 257 elements. In this paper, we consider a finite field that contains 257 elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules. The most common examples of finite fields are given by the integers modulo p when p is a prime number. For our case $\mathbb{Z}/p\mathbb{Z}$, $p = 257$.

We apply it to affine ciphers and show that this cipher looks like a permutation cipher. The idea based on this result, is to use the affine ciphers with the modulo 257 (as an initial permutation) in any specific algorithm of ciphering. Besides, one finishes with the decryption affine with the modulo 257 like an inverse permutation. This is to significantly increase the security of the specific encryption algorithm and to lengthen the 16-bits encryption key.

Keywords: Cryptography, Algebraic field, Primes, Affine cipher.

2010 Mathematics Subject Classifications: 11T71 (14G50), 06F25 (12J15), 11A41, 53B05, 14R05.

1 Introduction

The aim of Cryptography is to secure the transmission between the sender and the recipient. Securing information comes at many levels such that [1]:

- *Confidentiality:* Only the recipient (and possibly the sender) can understand the information transmitted,
- *Integrity:* Transmitted information has not been altered during its journey,
- *Authentication:* This is the act of proving an assertion, such as the identity of a computer system user,
- *Non-Repudiation:* It is the assurance that sender cannot deny the validity of information,
- *Access Control:* Only authorized people can access the information.

Confidentiality has long been obtained thanks to the knowledge of a secret common to the interlocutors (symmetric cryptography or secret key). The major disadvantage of this type of cryptography lies in the needing for a prior physical meeting between the interlocutors. So that, they agree on a secret allows them to communicate safely as reference [2]. The other aspects of security do not appear until much later with the advent of public key cryptography, which makes it possible to overcome the previous constraint.

A message M is a sequence of symbols out of an alphabet Σ [2, 3]. In cryptography, the encoding of message is called encrypting or ciphering. In the framework considered in this paper, encrypting will be done using a function E and a key K, which is itself a finite sequence of symbols out of an alphabet, usually but not necessarily the same as the message alphabet Σ.

In the current state of things such as encrypted multimedia data, mainly images and also text files are represented with extensions takes as pixels dimension and 8-bit characters. One can find a one-to-one function of these values and the elements of the set $\mathbb{Z}/256\mathbb{Z}$. In other words, the ciphering algorithms take results as modulo 256 values to size the images and the ciphered texts.

Then, the message alphabet [2] Σ is equal to a set $\Sigma = \{0, 1, 2, ..., 255\}$, and it is equivalent to the ring $\mathbb{Z}_{256}$ but, unfortunately, $\mathbb{Z}_{256}$ contains many zero-divisors. This ring is not recommended for use in cryptography, like, we will see during this paper.

With a small adjustment in our message alphabet Σ, we can introduce a new alphabet $\Sigma_1^* = \{1, 2, ..., 256\}$ or a set, and it's equivalent to the ring $\mathbb{Z}_{257} - \{0\}$, we significantly improve the robustness of these cryptosystem algorithms by introducing the number of 257 instead of 256.

2 Integral domain and field

These are two special kinds of ring [4, 5, 6]:

- If a, b are two ring elements with $a, b \neq 0$ but $ab = 0$ then a and b are called *zero-divisors*. In the ring $\mathbb{Z}_{256}$ we have $64 * 4 = 0$ and so 64 and 4 are zero-divisors. More generally, if n is not prime then $\mathbb{Z}_n$ contains zero-divisors.
- An *integral domain* is a commutative ring with an identity ($1 \neq 0$) with no zero-divisors. That is $ab = 0 \Rightarrow a = 0$ or $b = 0$. The ring $\mathbb{Z}$ is an integral domain.

A *field* is a commutative ring with identity ($1 \neq 0$) in which every non-zero element has a multiplicative inverse. The rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields. If a, b are elements of a field with $ab = 0$, then if $a \neq 0$ it has an inverse a^{-1} and so multiplying both sides by this gives $b = 0$.

Hence there are no zero-divisors and we have: *Every field is an integral domain.*

In mathematics, a finite field or Galois field is the set $\mathbb{F}p$ of mod-p remainders, where p is a given prime number. Here, as in $\mathbb{Z}_p$, the set of elements is $\mathbb{R}_p = \{0, 1, ..., p - 1\}$, and the operation $\oplus$ is (mod p) addition. The multiplicative operation $*$ is (mod p) multiplication, i.e., multiply integers as usual and then take the remainder after division by p.

Theorem 1. Suppose that n is a positive integer. Then the commutative ring $\mathbb{Z}/n\mathbb{Z} := \{0, 1, 2, ..., (n - 1)\}$ [4, 5, 6] is a field if and only if n is a prime number. Addition in this field is defined as adding a and b and then remainder (mod p). Multiplication is defined as multiplying a and b (mod p).

Theorem 2. Every finite integral domain is a field.

3 The role of prime 257

257 is a prime number. In Table 1 is given a list of all primes less than 260 [7, 8].

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**
A	2	3	5	7	11	13	17	19
B	23	29	31	37	41	43	47	53
C	59	61	67	71	73	79	83	89
D	97	101	103	107	109	113	127	131
E	137	139	149	151	157	163	167	173
F	179	181	191	193	197	199	211	223
G	227	229	233	239	241	251	**257**	~~263~~

Table 1. All primes less than 260

In general, $\mathbb{Z}_n$ has exactly n elements: $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$.

Theorem 3 ([7, 8]). Suppose that n is a positive integer. Then, the commutative ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is a field if n is a prime number. Conversely, if $\mathbb{Z}_n$ is a field, this implies that n is a prime number. $\mathbb{Z}_{257}$ is a field with elements which are taking values from 0 to 256. They are nonzero elements (the non-zero elements of 257 are the values from 1 to 256) and they are invertible. The inverse of 256 modulo 257 also equals to 256.

One have already a message alphabet Σ equal to a set $\Sigma = \{0, 1, 2, ..., 255\}$.

We can find a bijective function F between the non-zero values of 257 which are the numbers from 1 to 256 and the elements of the set of $\mathbb{Z} / 256\,\mathbb{Z}$.

$$F : \mathbb{Z}/256\mathbb{Z} \rightarrow (\mathbb{Z}/257\mathbb{Z})^*$$
$$\begin{cases} F(i) = i, & \forall i \neq 0 \\ F(0) = 256 \end{cases}$$

4 Affine cipher

An example of a cryptosystem which can benefit from this asset is the multiplicative Caesar cryptosystem or the affine encryption like in reference [1].

The affine encryption has the following function:

$$E(x) = ax + b \pmod{256}, \tag{2a}$$

such that a, b, x are integers and E is an affine function.

4.1 Adaptation of affine cipher in our case

The principle encryption function is

$$E(x) = a * x + b \pmod{257}, \tag{2b}$$

where a, b are keys for the affine cipher while x is a plaintext value [1].

4.2 Results and interpretations

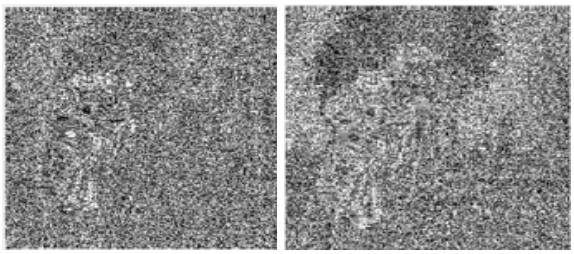
To validate the affine encryption, we take different values of a, b. In addition, we are working on grayscale images of 256 × 256 pixels, where each pixel can take a value between 0 and 255. We choose the 'Cameraman' and 'Lena' images in this dimension.

From Figures 1 and 2 it is seen that the affine encryption with modulo 257 makes a greater confusion in the plaintext image.

4.2.1 Entropy

Claude Shannon defined a function which is called as Shannon's entropy [9]. It is a mathematical function that corresponds to the amount of information contained in an information source. Entropy indicates, then, the amount of information necessary for the receiver to be able to unambiguously determine what the source has transmitted.

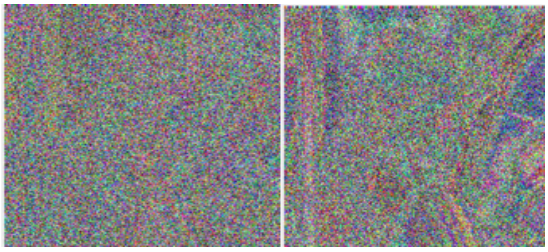
(a) (b)



(c) (d)

Figure 1. 'Cameraman' Image:
(a) Plaintext image,
(b) Encryption image with (a = 137, b = 0),
(c) Encryption image with (a = 97, b = 241),
(d) Encryption image with (a = 88, b = 120).

(a) (b)



(c) (d)

Fugure 2. 'Lena' Image:
(a) Plaintext image,
(b) Encryption image with (a = 137, b = 0),
(c) Encryption image with (a = 97, b = 241),
(d) Encryption image with (a = 88, b = 120).

For a source, which is a wide apart random variable X with n symbols, each symbol x_i having a probability P_i of appearing, the entropy H of the source X is given by

$$H(x) = -\sum_{i=1}^{n} P_i.\log_2(P_i)\,, \tag{3a}$$

we put

$$P_i = \frac{k_i}{n}\,, \tag{3b}$$

where i varies from 0 to 255, n is the number of values generated (n = 256 * 256 = 65536), and k_i corresponding to the frequency of each number i.

In general, we use a logarithm with base 2 because the entropy has the units of bit/symbol. The bits symbolize the probable achievements of the random variable X.

Let us consider a source consisting of an alphabet of 256 characters. If these characters are equiprobable, the entropy associated with each character is $\log_2(256) = \log_2(2^8) = 8$ bits (i.e. it takes 8 bits to transmit a character).

The ideal is to find the entropy of the encrypted image that approaches a source so that the source delivers equiprobable characters).

According to encryption function (Tables 2 and 3), the mean entropy of the encrypted 'Cameraman' image is 7.0062 bits (which corresponds to 99.95% of the entropy of the plaintext image) while the entropy of the encrypted 'Lena' image is 7.7452 bits (which corresponds to 99.93% of the entropy of the plain text image).

Encryption key		Plaintext image	Ciphering image
a	***b***		
137	0	7.0097	7.0097
97	241		7.0087
88	120		7.0002

Table 2. Entropy for ‘Cameraman’ image

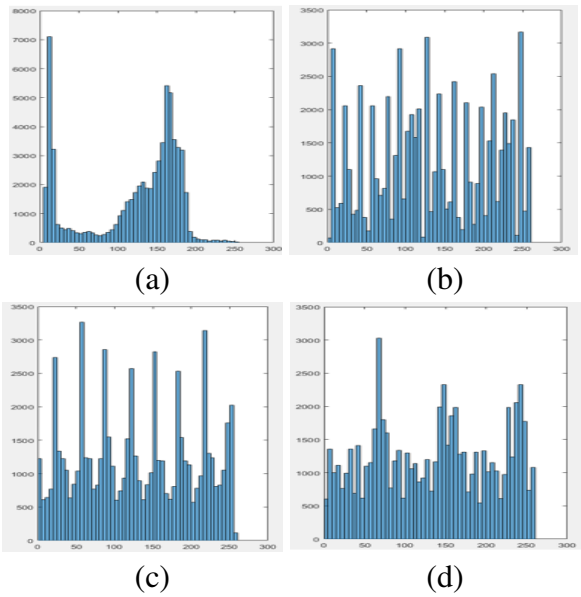
Encryption key		Plaintext image	Ciphering image
a	***b***		
137	0	7.7502	7.7502
97	241		7.7441
88	120		7.7413

Table 3. Entropy for ‘Lena’ image

The cipher-text has completely the same letter frequencies as the underlying plaintext. That is to say that the cipher may be identified as a transposition in lots of situations by the close resemblance of its letter statistics with the letter frequencies of the underlying language.

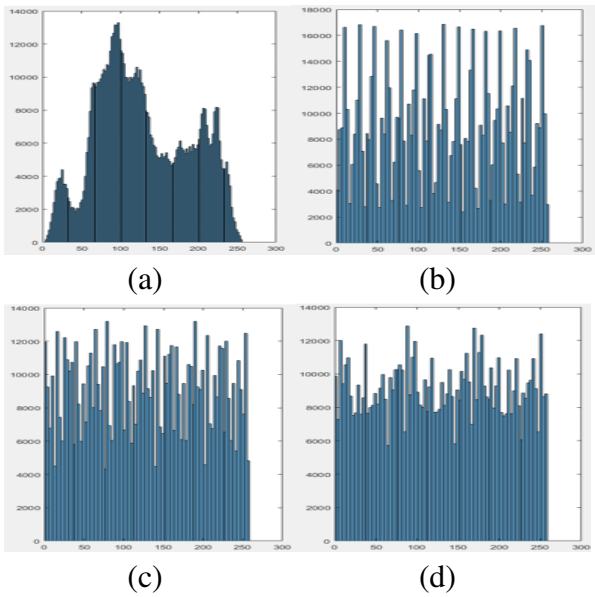
4.2.2 Histogram of images

For a monochrome image (it means that just with one component), the histogram is determined as a discrete function, which associates to each intensity value the number of pixels taking this value. Hence, the histogram is determined by counting the number of pixels for each intensity of the image. After that, the histogram can be seen as a probability density. Histograms are resistive to a number of transformations on the image of reference [9]. They are invariant to rotations, translations, and a lesser improve for changing in the perspective with scale.



(a) (b) (c) (d)

Figure 3. ‘Cameraman’ image:
(a) Plaintext image,
(b) Encryption image with (a = 137, b = 0),
(c) Encryption image with (a = 97, b = 241),
(d) Encryption image with (a = 88, b = 120).



(a) (b) (c) (d)

Figure 4. ‘Lena’ image:
(a) Plaintext image,
(b) Encryption image with (a = 137, b = 0),
(c) Encryption image with (a = 97, b = 241),
(d) Encryption image with (a = 88, b = 120).

We can clearly see that the plaintext image differs significantly from the corresponding encrypted image by referring to the results obtained (Figures 3 and 4).

Additionally, the histogram of the encrypted image is fairly uniform which makes it difficult to extract the statistical nature pixels from this image.

4.2.3 Adjacent pixel correlation

In the theory of probability and statistics, intensity of the link can exist between these variables to study the correlation between two random variables or numerical statistics. The link is an affine relationship, it is a linear regression. If we would like to give a numerical illustrate, we can calculate the correlation coefficient between two series of the same length (typical case: a regression).

The following tables of values are assumed as follows: $X(x_1, \ldots, x_n)$ and $Y(y_1, \ldots, y_n)$ and for each of the two series. A measure of the correlation is obtained by calculating the *Bravais–Pearson linear correlation coefficient* given in reference [9]. To know the correlation coefficient linking of these two series, we carry out the following equation:

$$Coeff(X,Y) = \frac{\operatorname{cov}(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}}, \tag{4}$$

The covariance between x and y is given by:

$$\operatorname{cov}(X,Y) = \frac{1}{N}\sum_{i=1}^{N}((X_i - E(X)).(Y_i - E(Y))). \tag{5}$$

The mean of X and Y are defined, respectively:

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} X_i, E(Y) = \frac{1}{N}\sum_{i=1}^{N} Y_i . \tag{6}$$

Besides, standard deviation of X and Y are obtained, respectively:

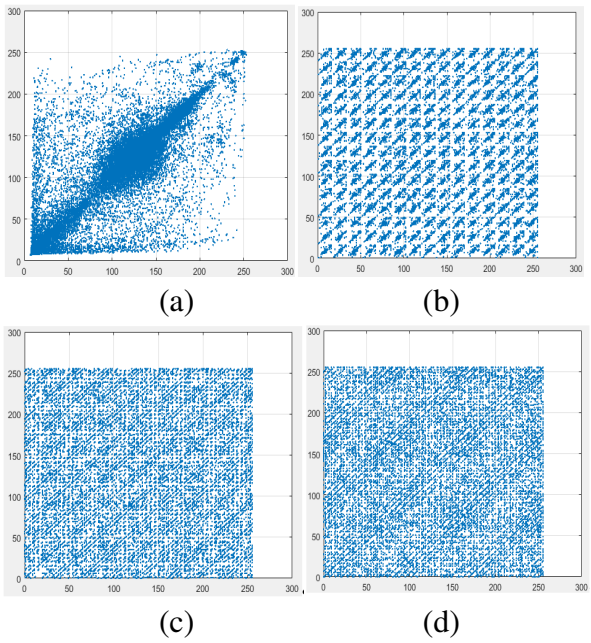
$$D(X) = \frac{1}{N}\sum_{i=1}^{N}(X_i - E(X))^2, D(Y) = \frac{1}{N}\sum_{i=1}^{N}(Y_i - E(Y))^2 . \tag{7}$$

The correlation coefficient is defined between −1 and 1. The intermediate values provide information on the degree of linear dependence between the two variables. The closer coefficient is to the extreme values −1 or 1, the stronger the correlation between the variables; the term "highly correlated" is simply used to describe the two variables. A correlation equal to 0 means that the variables are not correlated.

To test the correlation coefficient, we can choose *all pairs* of two adjacent pixels not only the clear image but also the encrypted image.

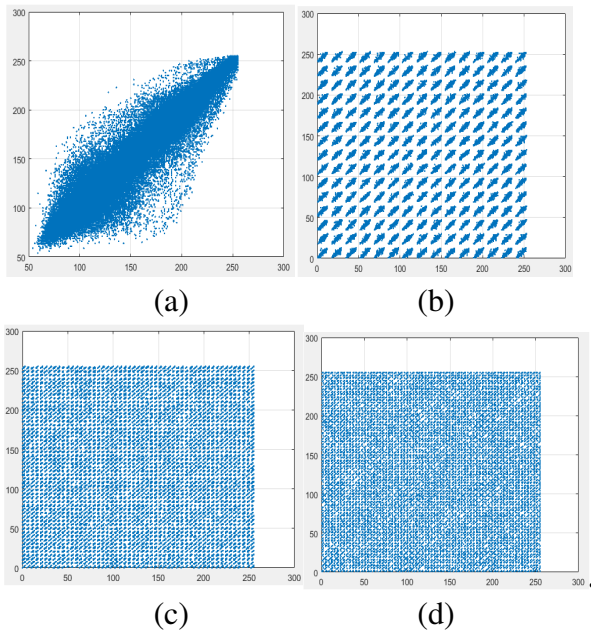
The four subfigures of Figure 5 represent the correlation between two horizontally adjacent pixels of the clear and ciphering images. It is seen that the neighbouring pixels have a strong correlation in the clear 'Cameraman' image (**Coeff = 0.93338**), while there is average correlation (**Coeff = 0.079164**) in the cipher.

This weak correlation between the two neighbouring pixels makes it difficult to assault our cryptography system in the encrypted image.



(a) (b) (c) (d)

Figure 5. ‘Cameraman’ image:
(a) Plaintext image,
(b) Encryption image with (a = 137, b = 0),
(c) Encryption image with (a = 97, b = 241),
(d) Encryption image with (a = 88, b = 120).



(a) (b) (c) (d)

Figure 6. ‘Lena’ image:
(a) Plaintext image,
(b) Encryption image with (a = 137, b = 0),
(c) Encryption image with (a = 97, b = 241),
(d) Encryption image with (a = 88, b = 120).

Encryption key		**Plaintext image**	**Ciphering image**
a	***b***		
137	0	0.93338	0.10536
97	241		0.047386
88	120		0.084746

Table 4. Correlation coefficient for the ‘Cameraman’ image

Encryption key		**Plaintext image**	**Ciphering image**
a	***b***		
137	0	0.99741	0.58774
97	241		0.58056
88	120		0.59449

Table 5. Correlation coefficient for the ‘Cameraman’ image

In addition, it is easily seen that several straight lines can be adjusted to this cloud of points in the clear image but among all these straight lines, we can retain the one that enjoys a spectacular property-giving rise to a straight line of the form $Y = aX + b$ thus presenting a *linear correlation.*

The four subfigures of Figure 6 represent the correlation between two horizontally adjacent pixels of the clear and ciphering image. It is seen that the neighbouring pixels in the clear ‘Lena’ image have a strong correlation (**Coeff = 0.99741**), while there is average correlation (**Coeff = 0.587596**) in the cipher.

4.3 Deciphering function

Let us consider

$$y = E(x) = ax + b \pmod{257}.$$

$$x = D(y) = \frac{y-b}{a} \pmod{257}. \tag{8a}$$

$$x = a^{-1} * (y-b) \pmod{257}. \tag{8b}$$

The inverse of a, is calculated by the extended Euclidean algorithm [1].

In the arithmetic and computer programming, the extended Euclidean algorithm also computes the greatest common divisor of integers a and 257 for the coefficients of Bézout's identity [1, 10] (which are integers u and v) such that:

$$a.u + 257v = \gcd(a, 257) = 1. \tag{9}$$

From (9) we get

$$au \cong 1 \pmod{257},$$

and it implies that u is the inverse of a for modulo 257. So, the deciphering function is given as follows:

$$x = u * (y + (257 - b)) \pmod{257}. \tag{10a}$$

$$x = u.y + c.c = u * (257 - b) \pmod{257}. \tag{10b}$$

5 Euler indicator function

In number theory [4, 5, 10], *Euler's totient function* counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter 'phi' as $\varphi(n)$ or $\phi(n)$, and may also be called Euler's phi function or *Euler Indicator*. In other words, it is the number of integers k in the range $1 \le k \le n$ for which the greatest common divisor gcd(n, k) is equal to 1. The integer k of this form is sometimes referred to as totatives of n.

For $n \in \mathbb{N}$, $\phi(n)$ = card{$k \in \{1, \ldots, n\}$, such as, gcd(n, k) = 1}

For example, there are eight totatives of 24 (1, 5, 7, 11, 13, 17, 19, and 23), so $\varphi(24) = 8$.

(1) If $n = p$, where p is prime number, then it is satisfied:

$$\phi(p) = p - 1, \quad \phi(1) = 1. \tag{11a}$$

(2) If $n = p^{\alpha}$ for prime number p and exponent α, then it is satisfied:

$$\phi(p^{\alpha}) = (p - 1).p^{\alpha-1}. \tag{11b}$$

n	$\phi(n)$	
$256 = 2^8$	$\phi(2^8) = (2-1).2^{8-1} = 2^7 =$	128
257	257 is first, then $\phi(257) = 257 - 1 =$	256

The complexity of the affine encryption increases from (128 * 256) values (possible key values if we work with modulo 256) to (256 * 256) values (possible keys if we work with modulo 257).

6 Conclusion

One can see in another way, that whole goal of this paper is to transform a finite set which contains zero-divisors to a set with no zero-divisors; which is an integral domain. It is clear that the fact of using 257 instead of 256, we double the capacity of the indicator of Euler.

An example of a cryptosystem which can benefit from this asset is the multiplicative Caesar cryptosystem or the affine encryption. The complexity of the affine encryption key ($E(x) = ax + b$), such that a and b form the key, x is the plaintext value and E is the affine cipher) increases from (128 * 256) with possible key values if we work on modulo 256 to (256 * 256) values possible keys if we work with modulo 257.

The idea based on this result, is to use the affine ciphers with the modulo 257, in any specific algorithm of ciphering and also one finishes with the decryption affine with the modulo 257 like an inverse permutation. This is to increase the security of the specific encryption algorithm and lengthen the 16-bits encryption key (8 bits for the value a, and 8 bits for the value b).

References

[1] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*, 794 pages, CRC Press, Taylor & Francis Group.

[2] Shannon, C. E. (1948). A Mathematical Theory of Communication, *The Bell System Technical Journal*, 27, pp. 379–423, 623–656, July, October, 1948.

[3] Bavaud, F., Chappelier, J.-C., & Kohlas, J. (2005). *An Introduction to Information Theory and Applications*. Available online: `https://www.coursehero.com/file/16418578/information-theory/` (Last viewed November 2020).

[4] Fieseler, K.-H. (2010). *Groups, Rings and Fields*, Uppsala.

[5] Savage, A. (2020). *Rings and Modules, Lecture notes*. Available at: `https://alistairsavage.ca/mat3143/notes/MAT3143-Rings_and_modules.pdf` (Last viewed November 2020).

[6] Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *An Introduction to Mathematical Cryptography*, Springer-Verlag New York.

[7] Desai, T. (2015). Application of Prime Numbers in Computer Science and the Algorithms Used To Test the Primality of a Number, *International Journal of Science and Research (IJSR)*, 4(9), 132–135, Paper ID: SUB157937.

[8] Languasco, A., & Perelli, A. (2003). Prime Numbers and Cryptography, In: *Emmer, M (Ed.) Mathematics and Culture*, Springer.

[9] Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos, Solitons and Fractals*, 21, 749–761.

[10] Easttom, C. (2016). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*, McGraw-Hill Education.