J. Appl. Math. & Informatics Vol. **39***(2021), No. 1 - 2, pp. 93 - 103*
https://doi.org/10.14317/jami.2021.093

GENERALIZED RSA CIPHER AND DIFFIE-HELLMAN PROTOCOL

ŁUKASZ MATYSIAK

Abstract. In this paper I am considering several cryptological threads. The problem of the RSA cipher, like the Diffie-Hellman protocol, is the use of finite sets. In this paper, I generalize the RSA cipher and DH protocol for infinite sets using monoids. In monoids we can not find the inverse, which makes it difficult. In the second part of the paper I show the applications in cryptology of polynomial composites and monoid domains. These are less known structures. In this work, I show different ways of encrypting messages based on infinite sets.

AMS Mathematics Subject Classification : 13P99, 13P25.
Key words and phrases : cryptology, decryption, encryption, RSA, protocol.

1. Introduction

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". The acronym RSA is the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, which was not declassified until 1997.[21]

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of the prime numbers can decode the message.[20] Breaking

Received June 10, 2020. Revised August 23, 2020. Accepted August 27, 2020. *Corresponding author.
© 2021 KSCAM.

RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

RSA is a relatively slow algorithm, and because of this, it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

More about the RSA cryptosystem can be found in many position, for example in [20], [7], [14].

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.[18], [9] DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Diffie–Hellman is used to secure a variety of Internet services. However, research published in October 2015 suggests that the parameters in use for many DH Internet applications at that time are not strong enough to prevent compromise by very well-funded attackers, such as the security services of large governments.[8]

The scheme was published by Whitfield Diffie and Martin Hellman in 1976,[9] but in 1997 it was revealed that James H. Ellis,[10] Clifford Cocks, and Malcolm J. Williamson of GCHQ, the British signals intelligence agency, had previously shown in 1969[24] how public-key cryptography could be achieved. [12]

Although Diffie–Hellman key agreement itself is a non-authenticated key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).

The method was followed shortly afterwards by RSA, an implementation of public-key cryptography using asymmetric algorithms.

Expired U.S. Patent 4,200,770 from 1977 describes the now public-domain algorithm. It credits Hellman, Diffie, and Merkle as inventors.

More about the RSA cryptosystem can be found in many position, for example in [18], [9], [8], [10], [24], [12].

In the section 3 I introduce generalized RSA. The problem of such a cipher is based on finite sets. Here I show it in infinite sets. Similarly in the section 5 Diffie-Hellman key exhange. In sections 7 and 9 I show applications of polynomial compositions and monoid domains to cryptology.

In sections 4, 6 and 8 we have examples.

2. Preliminaries

By a monoid, we mean a non-empty set M with an identity element and with one associative action $*\colon M \times M \to M$. If action $*$ is multiplication/addition, then this monoid is called multiplicative/additive.

Let's define the set of natural numbers as the set of positive integers and denote by $\mathbb{N}$, and by $\mathbb{N}_0$ the set of all non-negative integers. We see that $\mathbb{N}$ be a multiplicative monoid and $\mathbb{N}_0$ be an additive monoid.

Let's define the ideal of the monoid M. Set of the form $(a) = \{ma\colon m \in M\}$ ($a \in \mathbb{M}$) we call the ideal of the monoid M (in additive monoid $(a) = \{m+a\colon m \in M\}$). By the prime ideal we mean the ideal (p), where p is a prime element. Such ideal satisfies condition for any $a, b \in M$: if $ab \in (p)$ then $a \in (p)$ or $b \in (p)$. If $A = (a)$, $B = (b)$, where $a, b \in M$, then $AB = (a)(b) = (ab)$ is an ideal of M. If M is an additive monoid and $m, n \in M$ such that $m > n$, then $|(m)| < |(n)|$ and $(n)(\mathrm{mod}\ (m))$ is equal to ideal generated by $n(\mathrm{mod}\ m)$ (this is a normal congruence).

3. Generalized RSA cipher

We can assign an appropriate number to each letter of the alphabet: $A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7, I = 8, J = 9, K = 10, L = 11, M = 12, N = 13, O = 14, P = 15, Q = 16, R = 17, S = 18, T = 19, U = 20, V = 21, W = 22, X = 23, Y = 24, Z = 25$. So the alphabet is a finite set. The opposite side can easily decipher using the length of the alphabet. What if we extend this alphabet to an infinite set? In this situation, we can stay with the alphabet, but extend the length to infinity. So we have $A = 0 + 26k_0, B = 1 + 26k_1, C = 2 + 26k_2, \ldots, Y = 24 + 26k_{24}, Z = 25 + 26k_{25}$, where $k_0, k_1, \ldots, k_{25} \in \mathbb{N}_0$. So, for example, the text $ABACAB$ can be converted to 0 1 0 2 0 1, but also to 0 1 26 54 26 53. And we can give this number sequence to encrypt.

Generating keys

Let's choose distinct prime ideals $P = (p)$ and $Q = (q)$ (p, q are distinct primes) such that $N = PQ$ such that $|N| < |(x)|$, where x is the length of the alphabet.

Compute $\Phi(N) = (\varphi(n)) := (P-1)(Q-1) = (p-1)(q-1)$.

Let's choose the ideal $E = (e)$ such that e and $\varphi(n)$ are relatively primes $(\gcd(e, \varphi(n) = 1))$ and $|\Phi(N)| < |E| \subsetneq (1) = \mathbb{N}_0$.

We find the ideal $D = (d)$ such that $ED \equiv 1(\text{mod } \Phi(N))$.

The public key is defined as the pair of ideals (N, E), while the private key is the pair (N, D).

Encryption and decryption

We encrypt the message $M = M_0M_1 \dots M_r$ by calculation

$$C_i \equiv M_iE(\text{mod } \Phi(N))$$

.

The encrypted message $C = C_0C_1 \dots C_r$ is decrypted by formula

$$M_1 \equiv C_iD(\text{mod } \Phi(N)).$$

4. Example 1

Let's choose prime ideals (5) and (11) from $\mathbb{N}$. Hence $N = (55)$.

Compute $\Phi(N) = (\varphi(55)) := (4)(10) = (40)$.

Let's choose the ideal $E = (e)$ such that e and $\varphi(n)$ are relatively primes $(\gcd(e, \varphi(n) = 1))$ and $|\Phi(N)| < |E| \subsetneq (1) = \mathbb{N}_0$. For example $E = (13)$.

We find the ideal $D = (d)$ such that $ED \equiv 1(\text{mod } \Phi(N))$. We have $D \equiv (37)(\text{mod } (40))$.

The public key is defined as the pair of ideals (55) and (13), while the private key is the pair (55) and (37).

We have the English alphabet: $A = 00, B = 01, \dots, Z = 25$. So the length of this alphabet is 26.

We want to encrypt the message:
ALICE HAS A CAT.

Let's assign each letter an appropriate random value that satisfies the sign $+26t$, where $t \in \mathbb{N}$. In our example, we have the following transformation:

$$26116002043378720054 2619$$

We encrypt as follows:
$26E \equiv 26(13) \equiv (18)(\text{mod } (40))$
$11E \equiv 11(13) \equiv (23)(\text{mod } (40))$
...
$19E \equiv 19(13) \equiv (7)(\text{mod } (40))$.

We obtained the cryptogram:

$$18232026122914160022 1807$$

We decrypt the above ciphertext as follows:
$18D \equiv 18(37) \equiv (26)(\text{mod } (40))$
$23D \equiv 23(37) \equiv (11)(\text{mod } (40))$
...
$7D \equiv 7(37) \equiv (19)(\text{mod } (40))$.

We obtained an encrypted message:

$$261160020433787200542619 = ALICEHASACAT$$

5. Generalized Diffie–Hellman key exchange

First person F and second person S agree on the prime ideals (p) and (g) in $\mathbb{N}_0$ such that $|(p)| < |(g)|$.

Person F chooses any secret (a) in $\mathbb{N}_0$ and sends to person S

$$(A) \equiv (g)(a)(\text{mod } (p)).$$

Person S chooses any secret (b) in $\mathbb{N}_0$ and sends to person F

$$(B) \equiv (g)(b)(\text{mod } (p)).$$

Person F compute $(s) \equiv (B)(a)(\text{mod } (p))$.

Person S compute $(s) \equiv (A)(b)(\text{mod } (p))$.

Person F and person S share a secret ideal (s). This is because

$$(s) \equiv (g)(a)(b) \equiv (g)(b)(a)(\text{mod } (p)).$$

6. Example 2

Alice and Bob agree on the prime ideals (29) and (3) in $\mathbb{N}_0$.

Alice chooses any secret (23) in $\mathbb{N}_0$ and sends Bob

$$(A) \equiv (g)(a) \equiv (3)(23) \equiv (11)(\text{mod } (29)).$$

Bob chooses any secret (35) in $\mathbb{N}_0$ and sends Alice

$$(B) \equiv (g)(b) \equiv (3)(35) \equiv (18)(\text{mod } (29)).$$

Alice compute $(s) \equiv (B)(a) \equiv (18)(23) \equiv (8)(\text{mod } (29))$.

Bob compute $(s) \equiv (A)(b) \equiv (11)(35) \equiv (8)(\text{mod } (29))$.

Alice and Bob share a secret ideal $(s) = (8)$.

7. Applications of polynomial composites in cryptology

In 1976 [5] authors considered the structures in the form $D + M$, where D is a domain and M is a maximal ideal of ring R, where $D \subset R$. In [16] we could prove that in composite in the form $D + XK[X]$, where D is a domain, K is a field with $D \subset K$, that $XK[X]$ is a maximal ideal of $K[X]$. Next, Costa, Mott and Zafrullah ([6], 1978) considered composites in the form $D + XD_S[X]$, where D is a domain and D_S is a localization of D relative to the multiplicative subset S. In 1988 [4] Anderson and Ryckaert studied classes groups $D + M$. Zafrullah in [23] continued research on structure $D + XD_S[X]$ but he showed that if D is a GCD-domain, then the behaviour of $D^{(S)} = \{a_0 + \sum a_i X^i \mid a_0 \in D, a_i \in D_S\} = D + XD_S[X]$ depends upon the relationship between S and the prime ideals P od D such that D_P is a valuation domain (Theorem 1, [23]). Fontana and Kabbaj in 1990 ([11]) studied the Krull and valuative dimensions of composite $D + XD_S[X]$. In 1991 there was an article ([3]) that collected all previous composites and the authors began to create a theory about composites creating results. In this paper, the structures under consideration were officially called as composites. After this article, various minor results appeared. But the most important thing is that composites have been used in many theories as examples. That is why I decided to examine all possible properties of composites for commutative algebra. I put the first results in [16], and the next results in [17].

Consider A and B as rings such that $A \subset B$. Put $T = A + XB[X]$. The structure defined in this way is called a composite. (The definition comes from [3]).

I generalized the concept of a composite in two different directions.

Consider $A_0, A_1, \ldots, A_{n-1}$ and B be rings for any $n \geq 0$ such that $A_0 \subset A_1 \subset \cdots \subset A_{n-1} \subset B$. Put $T_n = A_0 + A_1X + \cdots + A_{n-1}X^{n-1} + X^nB[X]$.

And let other $A_0, A_1, \ldots, A_{n-1}$ and B be rings for any $n \geq 0$ such that there exists $i \in \{0, 1, \ldots, n-1\}$, where $A_i \not\subset A_{i+1}$ and for every $j \in \{0, 1, \ldots, n-1\}$ we have $A_j \subset B$. Put $T'_n = A_0 + A_1X + \cdots + A_{n-1}X^{n-1} + X^nB[X]$.

I have researched many properties in [16] and [17]. I will list the most important of them that may be related to this paper. In the following statements, for any structure A by A^* we mean a set of invertible elements of A.

Proposition 7.1. *Let $f = a_0 + a_1X + \ldots a_{n-1}X^{n-1} + a_nX^n + \cdots + a_mX^m \in T_n$ ($T_n = A_0 + A_1X + \cdots + A_{n_1}X^{n-1} + X^nB[X]$), where $0 \leq n \leq m$ and $a_i \in A_i$ for $i = 0, 1, \ldots, n$ and $a_j \in B$ for $j = n, n+1, \ldots, m$.*

(i) *$f \in T_n^*$ if and only if $a_0 \in A_0^*$ and $a_1, a_2, \ldots, a_m$ are nilpotents.*
(ii) *f is a nilpotent if and only if $a_0, a_1, \ldots, a_m$ are nilpotents.*

Proof. [16] Proposition 2.6. □

Theorem 7.2. *Consider $T = A + XB[X]$, where A be a subfield of B; $T_n = A_0 + A_1X + A_2X^2 \cdots + A_{n-1}X^{n-1} + X^nB[X]$, where $A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_{n-1} \subset B$ be fields. Then*

(i) *every nonzero prime ideal of T (T_n, respectively) is maximal;*
(ii) *every prime ideal P different from $XB[X]$ (in T) is principal;*
(iii) *every prime ideal P different from $A_1X + A_2X^2 + \cdots + A_{n-1}X^{n-1} + X^nB[X]$ (in T_n) is principal;*
(iv) *T is atomic, i. e., every nonzero nonunit of T is a finite product of irreducible elements (atoms);*
(v) *T_n is atomic.*

Proof. [16] Theorem 2.10. □

Since we are considering the properties of ACCP and atomicity, it is worth looking at the properties of GCD (greatest common divisor) and pre-Schreier.

Recall any unique factorization domain is GCD domain, and any GCD domain is pre-Schreier domain. But if assume atomic and pre-Schreier, then we have UFD.

Example 7.3. T, T_n (See Theorem 7.2) are no GCD-domains. Let $f = a_1 + b_1X, g = a_2 + b_2X$, where $a_1, a_2 \in A, b_1, b_2 \in B$ with $A + XB[X]$. Then $\gcd(f, g) = \dfrac{a_1b_2 - a_2b_1}{b_2}$. We see that $\gcd(f, g) \in B \setminus A$.

More information about GCD domains we can see in, e.g. [2], [19], [1].

Recall that a domain R is a pre-Schreier domain if every element $a \in R$ is a primal, i.e. for every elements $b, c \in H$ if $a \mid bc$ then there exist $a_1, a_2 \in R$ such that $a_1 \mid b, a_2 \mid c, a = a_1a_2$.

More information about Schreier and pre-Schreier domains we can see in many works, e.g. in [15], [19], [1], [22], respectively.

Lemma 7.4. *If $A \subset B$ be fields, then T be a pre-Schreier domain. If $A_0 \subset A_1 \subset \ldots A_{n-1} \subset B$ be fields, then T_n is also pre-Schreier domain.*

Proof. [16] Lemma 2.13. □

In [17] I consider composites with ACCP and atomic properties.

Each such polynomial is the sum of the products of the variable and the coefficient. And what if subsequent coefficient sets are appropriate cryptographic systems? Instead of encrypting with one system, we can create one system composed of many systems. Such a cipher is very difficult to break. If the spy detects encryption systems (composite coefficients), then the problem will be to find the right sum and product of such systems.

Assume that we have two people: Alice und Bob. Alice wants to send a message to Bob. Alice has one composite type T'_n and Bob has another one composite type T'_n.

We can build such composite by various encryption systems (even known ones). Let see note Lemma:

Lemma 7.5. *Let* $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + \sum_{j=n}^{m} a_jX^j$, $g = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + \sum_{j=n}^{m} b_jX^j \in T'_n$, *where* $a_i, b_i \in A_i$ *for* $i = 0, 1, \ldots, n-1$ *and* $a_j, b_j \in B$ *for* $j = n, n+1, \ldots m$. *Then*

$$fg \in A_0 + XB[X].$$

Put A_i, B_j $(i, j = 0, 1, \ldots, n-1)$ be different encryption systems. Then we have f and g are composition of encryption systems. No consider B. To improve security, let's fix that $\deg f = n-1, \deg g = n-k$, where $k \in \{2, \ldots n-1\}$. And such f, g Alice and Bob agree before the message is sent.

Alice and Bob multiply these composites to form one. We have $fg = (A_0 + A_1X + \ldots A_kX^k)(B_0 + B_1X + \cdots + B_lX^l) = A_0B_0 + (A_0B_1 + A_1B_0)X + \cdots + A_kB_lX^{k+l}$.

Note that the sum and product of the encryption systems must be defined in the formula above. Definitions we leave Alice and Bob. But in this section we can put $S_iS_j : x \to (x)_{S_i}(x)_{S_j}$ and $S_i + S_j : x \to ((x)_{S_i})_{S_j}$.

So in the product we encrypt the letter as two letters, the first in the first system and the second in the second system. And in the sum we encrypt the letter using the first system and then the second system. Of course, we can define completely different, at our discretion.

Assume that degree of fg is m and text to encrypt consists of more letters then $m+1$. Then we divide the text into blocks of length $m+1$. We can assume that $fg(0)$ encrypts the first letter of each block. Expression at X of fg encrypts the second letter of each block, and expression at X^2 of fg encrypts the third letter and so on.

Now, let's see how to decrypt in this idea.

Assume that we have an encrypted message $M_0M_1 \ldots M_n$. If our key is degree m, then we divide message on $m+1$ partition. And every partion divide to two. Every two letters are one letter of message.

Earlier we define $S_iS_j : x \to (x)_{S_i}(x)_{S_j}$ and $S_i + S_j : x \to ((x)_{S_i})_{S_j}$. Then decryption of two letters M_lM_{l+1} $(l = 0, 2, 4, \ldots)$ are $M_lM_{l+1} = (M_l)_{S_i}(M_{l+1})_{S_j} = N_{l,l+1}$ (one letter) and $M_l = ((M_l)_{S_i})_{S_j} = (N_l)_{ij}$ (one letter).

8. Example 3

Alice and Bob agree different encryption systems in the center: A_0, A_1, A_2, B_0, B_1. Next, Alice has gone far from Bob.

We have two compositions: $f = A_0 + A_1X + A_2X^2$, $g = B_0 + B_1X$. Their key is one composition in the form fg i.e.

$$A_0B_0 + (A_0B_1 + A_1B_0)X + (A_2B_0 + A_1B_1)X^2 + A_2B_1X^3.$$

The established systems are as follows:
A_0 is a Caesar cipher, where the letter is shifted one letter forward;
A_1 is a Caesar cipher, where the letter is shifted two letter forward;
A_2 is a Caesar cipher, where the letter is shifted three letter forward;
B_0 is a Caesar cipher, where the letter is shifted one letter back;
B_1 is a Caesar cipher, where the letter is shifted two letter back.

Suppose Alice wants to send a message saying

$$0 \quad 2 \quad 4 \quad 6 \quad 8 \quad 9 \quad 6 \quad 5$$

The degree of fg is 3. Hence message divide to $3+1$ partition. So the fourth letter is the same encrypted.

Letters 0 and 8 encrypt by A_0B_0. Then, from definition of A_0, B_0, 0 will be 1 9 (two letters). 8 will be 9 7.

Letters 2 and 9 encrypt by $A_0B_1 + A_1B_0$. Then 2 will be 5 9 and 9 will be 2 6.

Letters 4 and 6 encrypt by $A_2B_0 + A_1B_1$. Then 4 will be 9 1 and 6 will be 1 3.

Letters 6 and 5 encrypt by A_2B_1. Then 6 will be 9 4 and 5 will be 8 3.

Bob receives a message from Alice:

$$1 \quad 9 \quad 5 \quad 9 \quad 9 \quad 1 \quad 9 \quad 4 \quad 9 \quad 7 \quad 2 \quad 6 \quad 1 \quad 3 \quad 8 \quad 3$$

Now, Bob would like to read the message. Bob sees that message has 16 letters, so the original text has 8 letters, because the composition fg has degree 3 (i.e. $(3+1)2$ letters of original message). Divide message by 8 letters.

We take the first pairs from each section, i.e. 1 9 and 9 7. Bob uses decryption $(A_0B_0)^{-1}$. So, 1 will be 0 by A_0^{-1} and 9 will be 0 by B_0^{-1}. Hence 1 9 will be 0. Similarly, 9 7 will be 8.

Next, we take the second pairs from each section, i.e. 5 9 and 2 6. Bob uses decryption $(A_0B_1 + A_1B_0)^{-1}$. So, 5 9 will be 2 and 2 6 will be 9.

We take next pair, i.e. 9 1 and 1 3. Bob uses decryption $(A_2B_0 + A_1B_1)^{-1}$. So, 9 1 will be 4 and 1 3 will be 6.

Similarly, the last pairs decrypt by $(A_2B_1)^{-1}$. The pair 9 4 will be 6 and 8 3 will be 5.

After decrypting, Bob received the message:

$$0 \quad 2 \quad 4 \quad 6 \quad 8 \quad 9 \quad 6 \quad 5$$

9. The concept of using monoid domains in cryptology

Recall that if F be a field and M be a submonoid of $\mathbb{Q}_+$ then we can construct a monoid domain:

$$F[M] = F[X; M] = \{a_0X^{m_0} + \cdots + a_nX^{m_n} \mid a_i \in F, m_i \in M\}.$$

Any alphabet of characters creates a finite set. Most ciphers are based on finite sets. But we can have the idea of using the infinite alphabet $\mathbb{A}$, although in reality they can be cyclical sets with an index that would mean a given cycle. For example, A_0 - 0, B_0 - 1, ... , Z_0 - 25, A_1 - 0, B_1 - 1, ... , where A_i=A, ..., Z_i=Z for $i = 0, 1, \ldots$. We see that this is isomorphic to a monoid $\mathbb{N}_0$ non-negative integers by a formula

$$f\colon \mathbb{A} \to \mathbb{N}, f(m_i) = i.$$

Then we can use a monoid domain by a map

$$\varphi\colon \mathbb{A} \to F[\mathbb{A}], \varphi(m_0, m_1, \ldots, m_n) = a_0X^{m_0} + \ldots a_nX^{m_n}.$$

Here, one should think carefully about what a field F should be and think about additional mappings. In contrast, monoid domains can be excellent carriers of characters in the alphabet for monoids. This will make it harder to break any ciphers based on monoids for one simple reason, namely, we don't have inverse properties in a monoid.

References

1. D.D. Anderson, *GCD domains, Gauss' Lemma and contents of polynomials*, Chapman, S.T., Glaz, S. (eds.) Non-Noetherian commutative ring theory, Math. Appl., Kluwer, Dordrecht, **520** (2000), 1—31.
2. D.D. Anderson and D.F. Anderson, *Generalized GCD domains*, Comment. Math. Univ. St. Pauli, **28** (1979), 215—221.
3. D.D. Anderson, D.F. Anderson, and M. Zafrullah, *Rings between D[X] and K[X]*, Houston J. of Mathematics, **17** (1991), 109–129.
4. D.F. Anderson and A. Ryckaert, *The class group of $D + M$*, J. Pure Appl. Algebra, **52** (1988), 199–212.
5. J. Brewer and E. Rutter, *$D + M$ construction with general overrings*, Mich. Math. J., **23** (1976), 33–42.
6. D. Costa, J. Mott, and M. Zafrullah, *The construction $D + XD_S[X]$*, J. Algebra, **153** (1978), 423–439.
7. M. Cozzens and S. J. Miller, *The Mathematics of Encryption: An Elementary Introduction*, American Mathematical Society, (2013), p. 180.
8. A. David, *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*, (2015).
9. W. Diffie and M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, **22** 6 (1976), 644 – 654.
10. J.H. Ellis, *The possibility of Non-Secret digital encryption*, CESG Research Report, (2014).
11. M. Fontana and S. Kabbaj, *On the Krull and valuative dimension of $D+XD_S[X]$ domains*, J. Pure Appl. Algebra, **63** (1990), 231–245.

12. M.E. Hellman and E. Martin, *An overview of public key cryptography*, IEEE Communications Magazine, **40** 5 (2002), 42 – 49.
13. P. Jędrzejewicz, M. Marciniak, Ł. Matysiak and J. Zieliński, *On properties of square-free elements in commutative cancellative monoids*, Semigroup Forum, **100** (2020), 850–870.
14. N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Math., **114** Springer-Verlag (1987), p. 94.
15. S. McAdam and D.E. Rush, *Schreier Rings*, Bull. London Math. Soc., **10** (1978), 77–80.
16. Ł. Matysiak, *On properties of composites and monoid domains*, Accepted for printing in Advances and Applications in Mathematical Sciences, `http://lukmat.ukw.edu.pl/On%20properties%20of%20composites%20and%20monoid%20domains.pdf`, (2020).
17. Ł. Matysiak, *ACCP and atomic properties of composites and monoid domains*, Accepted for printing in Indian Journal of Mathematics, `http://lukmat.ukw.edu.pl/ACCP%20and%20atomic%20properties%20of%20composites%20and%20monoid%20domains.pdf`, (2020).
18. Merkle and C. Ralph, *Secure Communications Over Insecure Channels*, Communications of the ACM, **21** 4 (1978), 294 – 299.
19. G. Picavet, *About GCD domains*, Advances in commutative ring theory, in: Lect. Notes Pure Appl. Math., **205** (1999), 501–519.
20. R. Rivest, A. Shamir and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, **21** (2) (1978), 120 – 126.
21. N. Smart, *Dr Clifford Cocks CB*, Bristol University, (2008), Retrieved August 14, 2011.
22. M. Zafrullah, *On a property of pre-Schreier domains*, Comm. Algebra, **15** (1987), 1895–1920.
23. M. Zafrullah, *The $D + XD_S[X]$ construction from GCD-domains*, J. Pure Appl. Algebra, **50** (1988), 93–107.
24. *GCHQ trio recognised for key to secure shopping online*, BBC News, (2010).

Author received M.Sc. from Kazimierz Wielki University in Bydgoszcz and Ph.D at Nicolaus Copernicus University in Toruń. Since 2019 he has been at Kazimierz Wielki University. His research interests are polynomial composites (various algebraic properties, applications in Galois theory, geometry and economy) and cryptology.

Institute of Mathematics, Kazimierz Wielki University, Bydgoszcz 85-090, Poland.
e-mail: `lukmat@ukw.edu.pl`