ElGamal Public-Key Cryptosystem Using Reducible Polynomials Over a Finite Field

A. N. El-Kassar
Beirut Arab University, Mathematics Department, Beirut, Lebanon

Ramzi A. Haraty
Lebanese American University P.O.Box 13-5053 Chouran, Beirut, Lebanon 1102 2801

April 29, 2004

Abstract

The classical ElGamal encryption scheme is described in the setting of the multiplicative group \( \mathbb{Z}_p^\times \); the group of units of the ring of integers modulo a prime \( p \), but it can be easily generalized to work in any finite cyclic group \( G \). Among the groups of most interest in cryptography are the multiplicative groups \( \mathbb{F}_q^\times \) of the finite field \( \mathbb{F}_q \); these require finding irreducible polynomials \( h(x) \) over \( \mathbb{Z}_p \); for some prime \( p \); and constructing the quotient group \( \mathbb{Z}_p[x]/\langle h(x) \rangle = \mathbb{F}_q \).

Recently, El-Kassar et al. modified the ElGamal public-key encryption scheme from the domain of natural integers, \( \mathbb{Z} \), to the domain of Gaussian integers, \( \mathbb{Z}[i] \) by extending the arithmetic needed for the modifications in this domains.

The ElGamal public-key cryptosystem is extended to quotient rings of polynomials over finite fields having cyclic group of units. The major finding is that the quotient rings need not be fields. In particular, when \( p \) is an odd prime, a second degree reducible polynomial over \( \mathbb{Z}_p \) is used to easily implement the extended ElGamal public-key cryptosystems and to avoid finding irreducible polynomials.

1 Introduction

The ElGamal encryption scheme is typically described in the setting of the multiplicative group \( \mathbb{Z}_p^\times \); the group of units of the ring of integers modulo a prime \( p \), but it can be easily generalized to work in any finite cyclic group \( G \). The security of the generalized ElGamal encryption scheme is based on the intractability of the discrete logarithm problem in the group \( G \). The group \( G \) should be carefully chosen so that the group operations in \( G \) would be relatively easy to apply for efficiency. In addition, the discrete logarithm problem in \( G \) should be computationally infeasible for the security of the protocol that uses the ElGamal public key cryptosystem. The groups of most interest in cryptography are the multiplicative groups \( \mathbb{F}_q^\times \) of the finite field \( \mathbb{F}_q \), including the particular cases of the multiplicative groups \( \mathbb{Z}_p^\times \), and the multiplicative group \( \mathbb{F}_{2^m}^\times \) of the finite field \( \mathbb{F}_{2^m} \) of characteristic two, see [6]. Also of interest is the group of units \( \mathbb{Z}_n^\times \) where \( n \) is a composite integer such that \( n \) is 2, 4, \( p^t \), or \( 2p^t \), where \( p \) is an odd prime and \( t \) is an integer.
Gamal encryption scheme to the domain of Gaussian integers.

In [7], J. L. Smith and J. A. Gallian, determined the structure of the group of units of the quotient ring \( F_q[x] = \langle f(x) \rangle \) where \( f(x) \) is a polynomial in \( F_q[x] \). Using this decomposition, El-K assar et al. [4], gave a characterization of quotient rings of polynomials over \( \mathbb{F} \) with a cyclic group of units. The purpose of this paper is to use this classiﬁcation to apply ElGamal encryption scheme to the setting of \( \mathbb{F} \) over \( \mathbb{F} \)nite ﬁelds with a cyclic group of units. The characterization of quotient rings of polynomials

The rest of the paper is organized as follows: section 2 describes the classical ElGamal scheme. Section 3 presents the extension of ElGamal cryptosystem to the domain of Guassian integers. Section 4 presents the classiﬁcation of quotient rings of polynomials \( F_q[x] = \langle f(x) \rangle \) having cyclic group of units. Section 5 describes the extension of ElGamal cryptosystem to the domain of polynomial rings over a \( \mathbb{F} \)nite \( \mathbb{F} \)eld with cyclic group of units and section 6 presents a conclusion.

2 The Classical ElGamal Public Key Encryption Scheme

The classical ElGamal cryptosystem, see [2] and [6], can be described as follows. Let \( p \) be a large odd prime integer and let \( Z_p = \{0; 1; 2; 3; \ldots; p - 1\} \). Then, \( Z_p \) is a ring under addition and multiplication modulo \( p \). Since \( p \) is prime, \( Z_p \) is actually a \( \mathbb{F} \)eld under these operations. Moreover, \( Z_p^* = \{1; 2; 3; \ldots; p - 1\} \), the multiplicative group of the ring integers modulo \( p \), is a cyclic group generated by some generator \( \mu \) \( \in \mathbb{F} \) whose order is equal to \( p - 1 \). That is, every element of \( Z_p^* \) is a power of \( \mu \). Note that \( Z_p \) is a complete residue system modulo \( p \) and \( Z_p^* \) is a reduced residue system modulo \( p \). For further algebraic properties, see [5] and [6].

Suppose that entity B wants to send a message \( m \) to entity A. Entity B proceeds as follows: B gets the public key generated by A, then computes the ciphered message \( c = E_A(m) \) and sends it to A for decryption. To decipher it, A computes \( D_A(c) = m \).

3 ElGamal Public Key Cryptosystem In The Domain of Gaussian Integers

In [3], the ElGamal public key encryption scheme was extended to the domain of Gaussian integers \( \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}, 2 \leq z \} \). Algorithms and examples illustrating these modiﬁcations were given. The arithmetics in the domain of Gaussian integers were applied to extend the ElGamal cryptosystem as follows. Let \( \mathbb{G} \) be a Gaussian prime integer and let \( \mathbb{G} \) be a set of representatives of the elements of the quotient ring \( \mathbb{Z}[i] = \langle \mathbb{G}_0 \rangle \). Then, \( \mathbb{G} \) is a \( \mathbb{F} \)eld under addition and multiplication modulo \( \mathbb{G} \) having a cyclic multiplicative group \( \mathbb{G}^* \). Note that \( \mathbb{G}^* \) is a complete residue system modulo \( \mathbb{G} \) and \( \mathbb{G}^* \) is a reduced residue system modulo \( \mathbb{G} \). If \( \mathbb{G} = \frac{1}{2} \)
that the public-key is in a selected and note that there are m private key.
In order to generate the public-key, selects a random integer than p and in $\mathbb{G}^n$ is $\mathbb{A}(\overline{\mu}) = p^2 \overline{i} \cdot 1$. Hence, the cyclic group used in the extended ElGamal cryptosystem has an order larger than the square of that used in the classical ElGamal cryptosystem with no additional efforts required for nding the prime $p$. Now, a generator $\mu$ of $\mathbb{G}$ is selected and note that there are $\mathbb{A}(p^2 \overline{i} \cdot 1)$ generators in $\mathbb{G}^n$. Then a random positive integer a is chosen so that the public-key is $(p, \mu, \mu^a)$. Since $a$ is a power of $\mu$, then a must be less than the order of the group power $\mathbb{G}$ which is $p^2 \overline{i} \cdot 1$. This power of a is the private key.

To encrypt a message $m$, one rst represent it as an element $m$ in $\mathbb{G}$. Then, a random positive integer $k$ is selected to be used as a power so that $k$ is less than $p^2 \overline{i} \cdot 1$. The encrypted message is $c = (\overline{a}; \overline{d})$ where $\overline{a} = \overline{\mu}^k$ and $\overline{d} = \mathfrak{m} \overline{\mu}^k$: Note that the values of $\overline{a}$ and $\overline{d}$ must be elements of $\mathbb{G}$ and hence must be reduced modulo $\overline{\mu}$. The message $c$ is decrypted using the private key $a$ to compute $\overline{a}^i \overline{a}: \overline{c}$.

Example 2 In order to generate the public-key, entity A selects the Gaussian prime $\overline{\mu} = 359$ and a generator $\mu = 1 + 11i$ of $\mathbb{G}^n$: A chooses the private key $\mu = 86427$ and computes $\mu$ modulo $\overline{\mu}$: which is $\overline{\mu} = (1 + 11i)^{86427} \cdot 323 + 295i$ modulo 359. Therefore, A’s public-key is $(p = 359; \mu = 1 + 11i; \mu^a = 323 + 295i)$ and A’s private key is $a = 86427$: To encrypt the message $m = 101$, B selects a random integer $k = 115741$ and computes $\overline{a} = (1 + 11i)^{115741} \cdot 149 + 117i$ modulo 359 and $\overline{d} = 101(323 + 295i)^{115741} \cdot 147 + 209i$ modulo 359: Then B encrypts $\overline{a} = 149 + 117i$ and $\overline{d} = 147 + 209i$ to A. We note that B has 128880 choices for m in $\mathbb{G}^n$. Finally, A computes $\overline{a}^i \overline{a} = (149 + 117i)^{42453} \cdot 117 + 178i$ (mod 359); and recovers m by computing $(117 + 178i)^{(147 + 209i) \cdot 101}$ modulo 359:

4 Polynomial Rings Over a Field With Cyclic Group Of Units

The generalized ElGamal public key cryptosystem is usually studied in the setting of a finite field $\mathbb{F}_q$ and is based on working with the quotient ring $\mathbb{Z}_p[x] = \mathbb{H}(x); \mathbb{H}_q$ is an irreducible polynomial over $\mathbb{Z}_p[x]$; $q = p^n$; and $p$ is a prime integer. In the following, we extend the ElGamal public key cryptosystem to the setting of quotient rings of polynomials over a finite field $\mathbb{F}_q$ having a cyclic group of units where $\mathbb{H}(x)$ is not necessarily irreducible. It is well known that if $\mathbb{H}(x)$ is an irreducible polynomial of degree $n$; then $\mathbb{Z}_p[x] = \mathbb{H}(x)$ is a finite field of order $p^n$ and its nonzero elements form its cyclic group of units, $\mathbb{U}(\mathbb{Z}_p[x]) = \mathbb{H}(x)$; of order $\mathbb{U}(\mathbb{H}(x)) = 1$. Now consider the factor ring $\mathbb{F}_q[x] = < f(x) >$; where $\mathbb{F}_q$ is a finite field of order $q$ and $f(x)$ is a polynomial of degree $n$: Then $\mathbb{F}_q[x] = < f(x) > = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} : f_0, f_1, \ldots, f_{n-1} \in \mathbb{F}_q$. This ring is a ring whose elements are the congruence classes modulo $f(x)$ of polynomials in $\mathbb{F}_q[x]$ with a degree less than that of $f(x)$: Note that the representatives of the elements of $\mathbb{Z}_p[x] = \mathbb{H}(x) i$ form a complete residue system modulo $\mathbb{H}(x)$ in $\mathbb{Z}_p[x]$. Moreover, $\mathbb{Z}_p[x] = \mathbb{H}(x) i$ is a finite field of order $p^n$ and its nonzero elements form its cyclic group of units, $\mathbb{U}(\mathbb{Z}_p[x]) = \mathbb{H}(x) i$; of order $\mathbb{U}(\mathbb{H}(x)) = 1$.

Now consider the factor ring $\mathbb{F}_q[x] = < f(x) >$; where $\mathbb{F}_q$ is a finite field of order $q$ and $f(x)$ is a polynomial of degree $n$: Then $\mathbb{F}_q[x] = < f(x) > = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} : f_0, f_1, \ldots, f_{n-1} \in \mathbb{F}_q$. This ring is a ring whose elements are the congruence classes modulo $f(x)$ of polynomials in $\mathbb{F}_q[x]$ with a degree less than that of $f(x)$: For each irreducible polynomial $h(x)$ of degree $n$ over $\mathbb{F}_q$, the factor ring $\mathbb{F}_q[x] = < f(x) >$ is a finite field of order $q^n$: its group of units is isomorphic to the cyclic group $\mathbb{Z}_{q^n}$; in the case where $f(x)$ is not irreducible over $\mathbb{F}_q$, the quotient ring $\mathbb{F}_q[x] = < f(x) >$ is not a field. However, $f(x)$ can be selected so that the group of units of the quotient ring $\mathbb{F}_q[x] = < f(x) >$ is cyclic. This can be done by using the structure of the group of units of $\mathbb{F}_q[x] = < f(x) >$ was given by Smith and Gallian [7]. Before we summarize their results we recall the following well-known results. For a finite commutative ring $R$ with identity, we know from the fundamental theorem of finite abelian groups that $\mathbb{U}(R)$ is isomorphic to a direct product of cyclic groups. Also, if $R$
is a direct sum of rings then its group of units is isomorphic to the direct product of the corresponding group of units of each of the summands.

Theorem 3 If $R = R_1 \ast R_2 \ast \cdots \ast R_i$ then $U(R) \cong U(R_1) \times U(R_2) \times \cdots \times U(R_i)$.

Since $F_q[x]$ is a unique factorization domain, then $f(x)$ can be written as a product of powers of irreducible polynomials, $h_1(x)^{m_1}; h_2(x)^{m_2}; \ldots; h_k(x)^{m_k}$; in $F_q[x]$ and $F_q[x]=<f(x)> \cong F_q[x]=<h_1(x)^{m_1}> \ast \cdots \ast F_q[x]=<h_k(x)^{m_k}>$. In the case where $f(x)$ is not irreducible over $F_q$, theorem 1 can be applied and the problem reduces to that of finding the structure of $U(F_q[x]=<h(x)>)$; where $h(x)$ is irreducible over $F_q$. This result is stated as follows.

Lemma 4 If $f(x) = h_1(x)^{m_1}h_2(x)^{m_2}\cdots h_k(x)^{m_k}$, where all $h_i(x)$ are distinct irreducible polynomials in $F_q[x]$, then $U(F_q[x]=<f(x)> \cong U(F_q[x]=<h_1(x)^{m_1}> \times \cdots \times U(F_q[x]=<h_k(x)^{m_k}>)$.

The following theorems simplify the problem further.

Theorem 5 Let $F_q$ be a finite field and let $h(x)$ be an irreducible polynomial in $F_q[x]$. If $a$ is a root of $h(x)$ and $K = F_q(a)$, the extension of $F_q$ by $a$; then $F_q[x]=<h(x)> \cong K[x]=<x>$.

Theorem 6 Let $K$ be a finite field with $p^n$ elements, where $p$ is prime. Then, for any positive integer $m$, we have $U(K[x]=<x^m>) \cong \mathbb{Z}_{p^m}^* \times \mathbb{Z}_{p^m}$ where $s = \min \{ h_1 \geq 2 \} j h_1 \mid p^n$; $mg; k_i = \max \{ h_2 \mid h_1 > mg \}$ and $\mathbb{Z}_{p^m}$ occurs in the product $t$ times.

Note that the above lemma and theorems can be combined together to classify the group of units of any quotient ring of the form $F_q[x]=<f(x)>$.

Now we turn to the problem of classifying all quotient rings of polynomials $F_q[x]=<f(x)>$ with cyclic group of units. The results obtained in the remainder of this section are due to El-Kassar and Chehade, see [7]. If $h(x)$ is an irreducible polynomial over $F_q$ of degree $n$; we have that $F_q[x]=<h(x)>$ is a $\ast$-field of order $q^n = p^m$. Hence, $U(F_q[x]=<h(x)>)$ is cyclic with order $q^n - 1 = p^m - 1$ and $U(F_q[x]=<h(x)>) \cong \mathbb{Z}_{p^m - 1}$. Next we consider the case where $f(x)$ is a power of an irreducible polynomial $h(x)$; that is $f(x) = h(x)^m$. We note that if $h(x)$ is of degree 1, then $F_q[x]=<h(x)> \cong \mathbb{Z}_{p^m}^* \times \mathbb{Z}_{p^m}$. Also note that in order for $U(F_q[x]=<x^m>) \cong \mathbb{Z}_{p^m}^* \times \mathbb{Z}_{p^m}$, $x = h(x)^m$ is irreducible.

Theorem 7 Let $F_q$ be a finite field of order $q = p^2$; where $p$ is a prime integer, and let $h_i(x)$ be irreducible factor of $f(x)$ in $F_q[x]$ with $\deg h_i(x) = q_i$. Then, $U(F_q[x]=<f(x)>)$ is cyclic if and only if one of the following is true:

i- $f(x)$ is irreducible and $U(F_q[x]=<f(x)>) \cong \mathbb{Z}_{p^2}$.

ii- $f(x) = h(x)^2$ and $U(F_q[x]=<f(x)>) \cong \mathbb{Z}_{p^2}^*$ where $h(x)$ is linear and $F_q \cong \mathbb{Z}_p$.

iii- $f(x) = h_1(x):h_2(x)\cdots h_k(x)$ where $q = 2$. The $c_i$s are pairwise relatively prime and $U(F_q[x]=<f(x)>) \cong \mathbb{Z}_{2^e_1} \times \mathbb{Z}_{2^e_2} \times \cdots \times \mathbb{Z}_{2^e_j}$.

iv- $f(x) = h_1(x):h_2(x)\cdots h_k(x)^2$ where $q = 2$. The $c_i$s are pairwise relatively prime, $h_i(x)$ is linear and $U(F_q[x]=<f(x)>) \cong \mathbb{Z}_{2^{e_1}} \times \mathbb{Z}_{2^{e_2}} \times \cdots \times \mathbb{Z}_{2^{e_j}}$.

5 ElGamal Public Key Cryptosystem over Quotient Rings of Polynomials over Finite Fields

Now we describe the extended ElGamal encryption scheme over quotient rings of polynomials $Z_p[x]=h(x)i$ where $h(x)$ is reducible. From the above study we conclude that in order for the group of units $U(Z_p[x]=h(x)i)$; where $p$ is an odd
prime, to be cyclic, h(x) must be a square power of only one linear irreducible polynomial. That is, \( h(x) = h_1(x)^2 \), where \( h_1(x) = ax + b \). This means that \( \text{U}(\mathbb{Z}_p[x] = (ax + b)^2) \) is cyclic. But, \( \mathbb{Z}_p[x] = (ax + b)^2 \cong \mathbb{Z}_p[x] = < x^2 > \). Hence, we can extend the ElGamal scheme in the setting of the group of units of the ring \( \mathbb{Z}_p[x] = < x^2 > \), of order \( A(x^2) = p(p_1 1) \). We note that a polynomial \( f(x) \) in \( \mathbb{Z}_p[x] \) belongs to the cyclic group \( \text{U}(\mathbb{Z}_p[x] = (x^2)) \) if and only if \( f(x); x = 1 \). This is equivalent to say that \( x \) does not divide \( f(x) \), where \( f(x) \) is a linear polynomial. Hence, \( \text{U}(\mathbb{Z}_p[x] = (x^2)) = \{ f \in \mathbb{Z}_p[x]; f(x) = x + 1 \} \). The extended ElGamal cryptosystem in this setting is given next through three algorithms.

First, to generate the corresponding public and private keys, entity A should use the following algorithm:

**Algorithm 8 (Key generation)**

1. Generate a large random prime \( p \) and a reducible polynomial \( h(x) \) in \( \mathbb{Z}_p[x] \) as a square of a linear polynomial and compute \( A(x^2) = p(p_1 1) \).

2. Find a generator \( \oplus(x) \) of the multiplicative group \( \text{U}(\mathbb{Z}_p[x] = (x^2)) \). That is, \( \text{U}(\mathbb{Z}_p[x] = (x^2)) = \{ f \in \mathbb{Z}_p[x]; \oplus(x) \} \).

3. Select a random integer \( a, 2 \cdot a \cdot A(x^2); i \); \( A(x^2); i \); 1: Note that the integer \( a \) should be a natural integer in the interval \( [2; p^2 \cdot p_1 2] \).

4. Compute \( \oplus(x)^a \pmod {x^2} \).

5. A’s public key is \( (p; x^2; \oplus(x); \oplus(x)^a) \); A’s private key is \( a \).

To encrypt a message \( m(x) \) \( 2 \mathbb{Z}_p[x] = (x^2) \), entity B should use the following algorithm:

**Algorithm 9 (Encryption scheme)**

1. Obtain A’s authentic public key \( (p; x^2; \oplus(x); \oplus(x)^a) \).

2. Select a random integer \( k, 2 \cdot k \cdot A(x^2); i \); 1:

3. Represent the message as a polynomial \( m(x) \) \( 2 \mathbb{Z}_p[x] = (x^2) \).

4. Compute \( \phi(x) = \oplus(x)^k \pmod {x^2}; \phi(x)^k \), and \( \phi(x) \cdot m(x); \phi(x)^a_k \pmod {x^2} \).

5. Send the ciphertext \( \phi(x), \phi(x) \) sent by entity B; entity A should use the following algorithm:

**Algorithm 10 (Decryption scheme)**

1. Receives the ciphertext \( \phi(x), \phi(x) \) sent by entity B.

2. Use the private key \( a \) to compute \( \phi(x)^a \pmod {x^2} \).

3. Recover the plaintext \( m(x) \) by computing \( \phi(x)^a \pmod {x^2} \).

The following theorem proves that the decryption formula \( \phi(x)^a \pmod {x^2} \) allows the recovery of the original plaintext \( m(x) \).

**Theorem 11** Given a generator \( \oplus(x) \) of the multiplicative group of the polynomial \( \mathbb{Z}_p[x] = (x^2) \); then \( \phi(x) \) and \( \phi(x) \) as in the algorithms such that \( \phi(x) = \oplus(x)^a \pmod {x^2} \) and \( \phi(x) = m(x); \phi(x)^a \pmod {x^2} \). Let \( s(x) = \phi(x)^a \pmod {x^2} \), then \( m(x) = s(x) \).

Proof. Since \( \phi(x) = \oplus(x)^a \pmod {x^2} \), where \( \oplus(x) \) is a generator of the multiplicative group \( \text{U}(\mathbb{Z}_p[x] = (x^2)) \), it follows that \( \phi(x) \) is in \( \text{U}(\mathbb{Z}_p[x] = (x^2)) \) so that \( \phi(x); x^2 = 1 \). Therefore, using a version of Fermat’s little theorem for polynomials over an infinite field, we have that \( \phi(x)^{(p_1 1)} = 1 \cdot 1 \pmod {x^2} \). Then, \( \phi(x)^{(p_1 1)} \cdot \phi(x)^a \pmod {x^2} \) and thus \( \phi(x)^a \pmod {x^2} \).

Example 12 For \( p = 3; U(\mathbb{Z}_3[x] = (x^2)) = f; 1 \cdot 2; 1 + x; 2 + x; 1 + 2x; 2 + 2x \text{ and } A(x^2) = 6 \). Note that \( x^2 \) is the zero in \( \mathbb{Z}_3[x] = (x^2) \). To nd a generator to \( U(\mathbb{Z}_3[x] = (x^2)) \), select the polynomial \( \oplus(x) = \)
2 + x in \( U(\mathbb{Z}_3[x]) = \langle x^2 \rangle \). The order \( \mathbb{A}(x^2) = 6 \) has two prime divisors 2 and 3: Since \((2 + x)^2 = 4 + 4x + 4x^2 = 4 + 4x + 1 + x \) \( \mathbf{6} \) \( 1 \) over \( \mathbb{Z}_3 \) and \((2 + x)^3 = 2 + 3x + x^2 \) \( 2 \) \( \mathbf{6} \) \( 1 \) over \( \mathbb{Z}_3 \): Hence, \( \mathbb{A}(x) = 2 + x \) is a generator. To generate the corresponding public and private keys, entity A should …rst choose its own private key \( a = 4 \), then computes \( \mathbb{A}(x)^a = \mathbb{A}(x)^4 = (2 + x)^4 \cdot 1 + 2x \) \( \mod x^2 \). Thus, \( \mathbb{A}(x) \)'s private key is \( a = 4 \) and public key is \((3; x^2; 2 + x; 1 + 2x)\). To encrypt the message \( m(x) = 2x + 2 \), entity B selects randomly an integer \( k = 3 \); then computes \( \mathbb{c}(x) = \mathbb{A}(x)^k = (2 + x)^3 \cdot 2 \) \( \mod x^2 \) \( \mod x^2 \) and \( \mathbb{d}(x) = m(x);(\mathbb{A}(x)^a)^k = (2x + 2);(2x + 2)^3 \cdot 2 + 2x \) \( \mod x^2 \). The ciphertext is \( \mathbb{c}(x) = (\mathbb{c}(x); \mathbb{d}(x)) \). Hence, entity B sends the ciphertext \((2; 2x + 2)\) to entity A. To decrypt the sent ciphertext \((2; 2x + 2)\), entity B should use its own private key \( a = 4 \) to compute \( \mathbb{c}(x)^i \cdot \mathbb{c}(x)^a: \mathbb{d}(x) = (2)^4 \cdot 1 \) \( \mod x^2 \). Finally, the plaintext \( m(x) \) can be recovered by computing \( s(x) = \mathbb{c}(x)^i \cdot \mathbb{c}(x)^a: \mathbb{d}(x) \cdot 1:2x + 2 = 2x + 2 \) \( \mod x^2 \).

### 6 Conclusion

Using a characterization of quotient rings of polynomials over \( \mathbb{Z} \) with a cyclic group of units, the ElGamal encryption scheme was extended to the setting of \( F_p[x] = \langle x \rangle \) where \( f(x) \) is a reducible polynomial in \( F_p[x] \); Algorithms for the extended ElGamal cryptosystem in the setting of \( \mathbb{Z}_p[x] = \langle x^2 \rangle \) were given along with their proofs. A numerical example was provided to illustrate the new method.

We conclude this paper by considering the following problem. In addition to the new setting, \( \mathbb{Z}_p[x] = \langle x^2 \rangle \), where \( p \) is an odd prime, one may consider the case of extending ElGamal public-key cryptosystem using the reducible polynomials in cases (iii) and (iv) of theorem 7. Note that in this case one needs to …nd irreducible polynomials over \( \mathbb{Z}_2 \); unlike the case considered in this paper. Also note that if \( p \) is an odd prime of the form \( 4k + 1 \); then \( \mathbb{Z}_p[x] = \langle x^2 \rangle \) is not reduced to the classical case and when \( p \) is of the form \( 4k + 3 \); one may use either the setting \( \mathbb{Z}_p[x] = \langle x^2 \rangle \) or \( \mathbb{Z}[i] = \mathbf{1} \mathbf{p} \) which are basically different:

### References


This work is funded by the Lebanese American University