УДК 004.056.5

РОЗРОБКА ДЕМОНСТРАЦІЙНОГО ДОДАТКУ ДЛЯ ФОРМУВАННЯ СПІЛЬНОГО СЕКРЕТНОГО КЛЮЧА З ВИКОРИСТАННЯМ ПРОТОКОЛУ ДІФФІ-ХЕЛМАНА НА ЕЛІПТИЧНИХ КРИВИХ

Драна Наталя, Пузікова Анна

Науковий керівник: канд. фіз.-мат. наук, доцент Пузікова А.В.

Центральноукраїнський державний педагогічний університет імені Володимира Винниченка, м. Кропивницький, Україна

Стрімкий розвиток криптографії на еліптичних кривих призводить до необхідності формування у студентів спеціальності «122 Комп'ютерні науки» розуміння непростого математичного апарату теорії еліптичних кривих над скінченими полями та принципів еліптичної криптографії, які використовуються в сучасних криптографічних стандартах. Тому розробка відповідного демонстраційного додатку є актуальною задачею для вирішення освітніх потреб під час вивчення відповідних тем курсу «Інформаційна безпека та криптографія». У статті стисло викладено частину результатів розробки демонстраційного додатку для формування спільного секретного ключа з використанням протоколу Діффі-Хелмана на еліптичних кривих.

Ключові слова: демонстраційний додаток, криптографія на еліптичних кривих, протокол Діффі-Хелмана на еліптичних кривих.

DEVELOPMENT OF A DEMONSTRATION APPLICATION FOR GENERATING A SHARED SECRET KEY USING THE DIFFIE-GELLMAN PROTOCOL ON ELLIPTIC CURVES

Drana Natalia, Puzikova Anna

Scientific adviser: Candidate of Physical and Mathematical Sciences Puzikova A.V.

Volodymyr Vynnychenko Central Ukrainian State Pedagogical University, Kropyvnytskyi, Ukraine

The rapid development of Elliptic Curve Cryptography leads to the need for students of the specialty "122 Computer Sciences" to develop an understanding of the complex mathematical apparatus of elliptic curve theory over finite fields and the principles of elliptical cryptography used in modern cryptographic standards. Therefore, the development of an appropriate demonstration application is an urgent task for the solution of educational needs in the study of relevant topics of the course "Information Security and Cryptography".

The article briefly describes some of the results of the development of a demo application for generating a shared secret key using the Elliptic curve Diffie–Hellman.

Keywords: demo application, Elliptic Curve Cryptography, Elliptic curve Diffie–Hellman.

Постановка проблеми. Одним із сучасних напрямів розвитку криптографічних методів, які забезпечують захист інформаційних ресурсів, їх безпечну обробку та зберігання, а також передачу інформації, є криптографія на еліптичних кривих (Elliptic Curve Cryptography, ECC), використання яких у криптосистемах з відкритими ключами вперше було запропоновано незалежно один від одного Нілом Кобліцем (Neal Koblitz) та Віктором Міллером (Victor Miller) у 1985 році.

Криптографія на еліптичних кривих отримала свій розвиток у роботах таких вчених: Bernstein D., Edwards H., Koblitz N., Menezes A., Washington L., Lange T., Горбенко І.Д., Бессалов А.В., Ковальчук Л.В., Корнейко О.В., Кочубинський А.І., Чевардін В.Є. та ін.

Використання еліптичних кривих для вирішення такої криптографічної задачі, як формування цифрового підпису, було закріплено в американських стандартах Національним інститутом стандартів і технологій США у 1998 році, а у 2002 році в Україні ухвалено стандарт цифрового підпису ДСТУ 4145–2002, який ґрунтується на еліптичних кривих.

У порівнянні з поширеними в останні десятиліття криптосистемами, такими як RSA (криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел), криптографія на еліптичних кривих пропонує рівноцінний захист разом із істотно меншими розмірами ключів. Зменшення розмірів ключів відповідно призводить до економії енергії, пам'яті, пропускної здатності та обчислювальних витрат [3], що надає ECC істотні переваги над більшістю інших криптографічних підходів.

Так, криптографія на еліптичних кривих використовується в протоколах захисту транспортного рівня (TLS), зокрема у мобільних (бездротових) середовищах [3], а також у протоколі транспортного рівня SSH [2]. Останній використовує протокол Діффі-Хелмана на еліптичних кривих (Elliptic curve Diffie–Hellman, ECDH) для формування спільного секретного ключа та алгоритм з відкритим ключем для створення цифрового підпису на основі

еліптичних кривих (Elliptic Curve Digital Signature Algorithm, ECDSA) [6]. Інше застосування ECC здобула у протоколі OpenPGP [4], який підтримує такі стандарти алгоритмів з відкритим ключем, як RSA та DSA (Digital Signature Algorithm, криптографічний алгоритм з використанням відкритого ключа для створення електронного підпису).

Одним із нових українських стандартів, у якому використовується ECC, є «ДСТУ 9041:2020. Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса» [1].

Таким чином, зважаючи на поширений інтерес до криптографії на еліптичних кривих серед науковців та практиків, а також необхідність формування у студентів розуміння непростого математичного апарату теорії еліптичних кривих над скінченими полями та принципів еліптичної криптографії, які використовуються в сучасних криптографічних стандартах, розробка демонстраційного навчального додатку для формування секретного ключа з використанням протоколу Діффі-Хелмана на еліптичних кривих є актуальною задачею для вирішення освітніх потреб під час вивчення відповідних тем курсу «Інформаційна безпека та криптографія».

Метою статті є стислий виклад частини результатів розробки демонстраційного додатку для формування спільного секретного ключа з використанням протоколу Діффі-Хелмана на еліптичних кривих.

Основними завданнями створення додатку є такі:

- надати користувачеві можливість переглядати теоретичні відомості про поняття та рівняння еліптичної кривої, доповнивши їх візуалізацією тривимірного тіла, заданого певним рівнянням, та відображення зрізів цього тіла на площині;
- інтерактивне моделювання процесу виконання операції додавання і множення на натуральне число точок еліптичної кривої над полем дійсних чисел з відповідним графічним відображенням (рис.1);

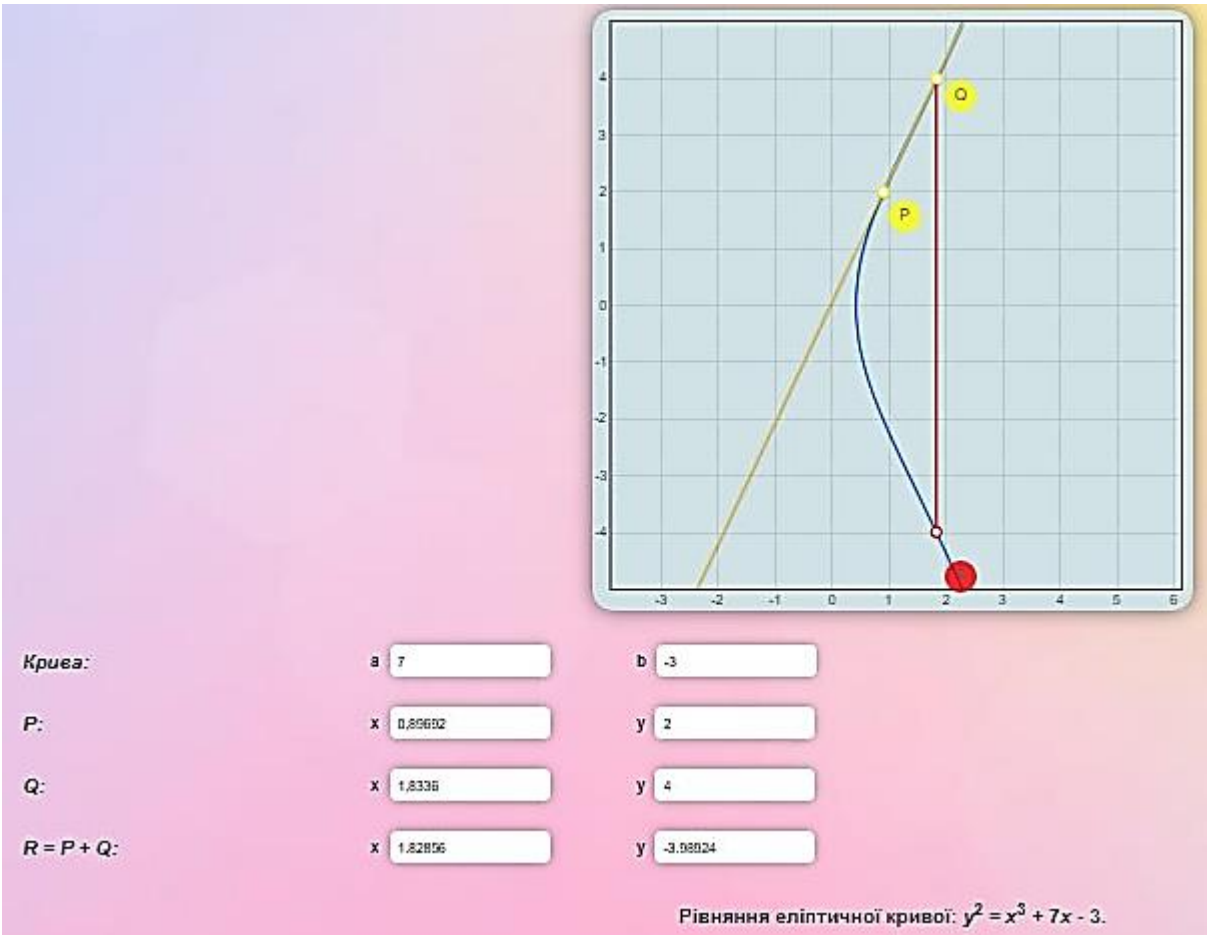

Рис 1. Веб-сторінка, яка демонструє процес виконання операції додавання точок еліптичної кривої над полем дійсних чисел

- інтерактивне моделювання процесу виконання операції додавання і множення на натуральне число точок еліптичної кривої над полем Галуа, відображення відповідних точок на площині та підрахунок їх кількості;
- моделювання процесу формування спільного секретного ключа з використанням протоколу Діффі-Хелмана на еліптичних кривих (рис. 2).

Зокрема, для розв'язання останнього з перелічених вище завдань, у демонстраційному додатку засобами Vue.js була реалізована веб-сторінка з такою структурою (рис. 2):

- блок з формою, що містить поля для введення коефіцієнтів рівняння еліптичної кривої, а також саме це рівняння, сформоване відповідно до заданих користувачем значень коефіцієнтів;
- блок з формою, що приймає на вхід секретні коефіцієнти α та β Аліси і Боба відповідно, а також повертає результати проміжних розрахунків $Q(A) = \alpha *$

P – для Аліси та $Q(B) = \beta * P$ – для Боба, які передаються незашифрованим каналом зв’язку;

– блок з формою, на якій відображено результати обрахунків $\alpha * Q(B)$ – для Аліси та $\beta * Q(A)$ – для Боба, тобто координати точки еліптичної кривої, абсциса якої може бути використана Алісою і Бобом як спільний секретний ключ.

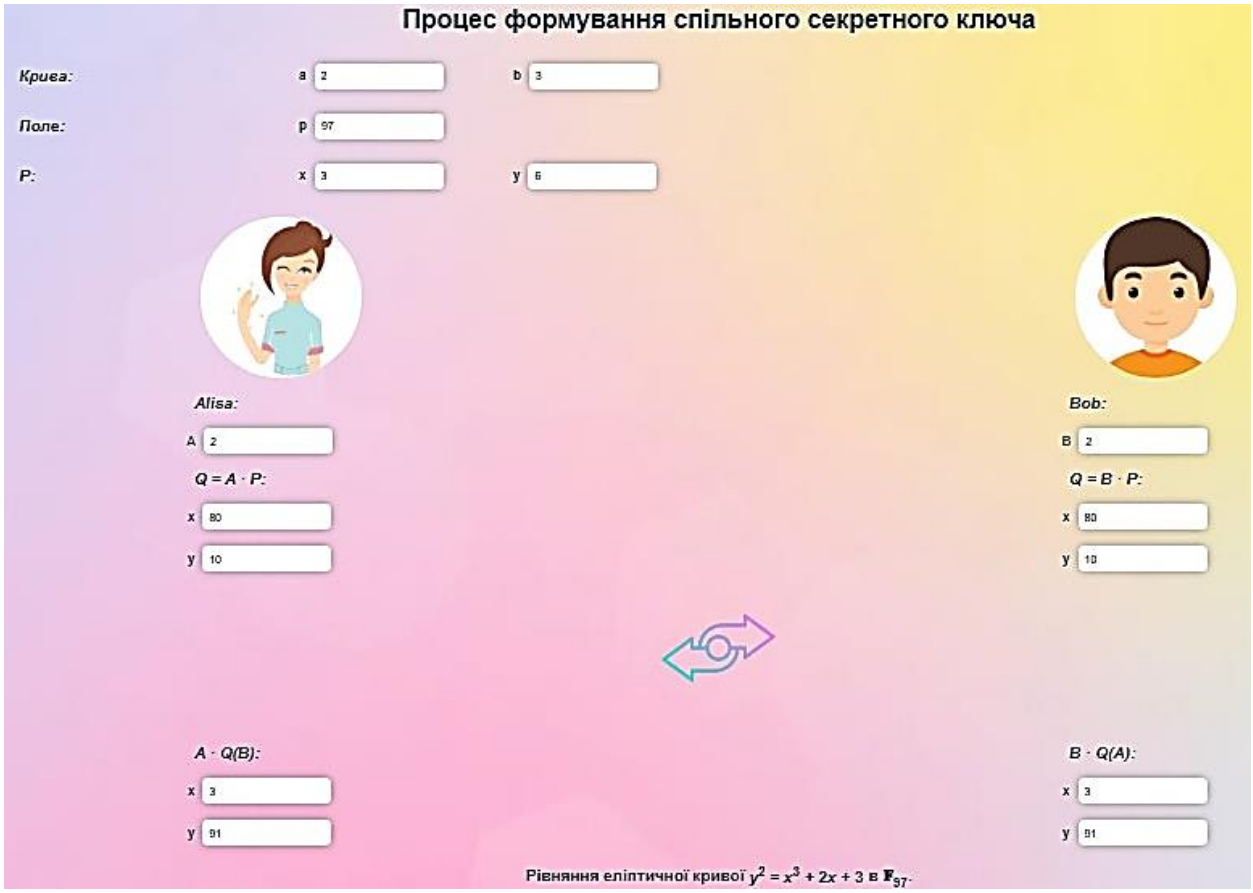

Рис 2. Веб-сторінка, яка демонструє процес формування спільного секретного ключа з використанням протоколу Діффі-Хелмана на еліптичних кривих

Виконання основних обчислень було реалізовано у функції *addPoints()*, код якої наведено нижче:

```
$.ec.modk.Base.prototype.addPoints = function( p1, p2 ) {
        if( p1 === null ) {
            return p2;
        }
        if( p2 === null ) {
            return p1;
        }
        var x1 = p1[ 0 ];
```

```
        var y1 = p1[ 1 ];
        var x2 = p2[ 0 ];
        var y2 = p2[ 1 ];
        var m;
        if( x1 !== x2 ) {
            m = ( y1 - y2 ) * this.inverseOf( x1 - x2 );
        }
        else {
            if( y1 === 0 && y2 === 0 ) {
                return null;
            }
            else if( y1 === y2 ) {
                m = ( 3 * x1 * x1 + this.a ) * this.inverseOf( 2 * y1 );
            }
            else {
                return null;
            }
        }
        m %= this.k;
        var x3 = ( m * m - x1 - x2 ) % this.k;
        var y3 = ( m * ( x1 - x3 ) - y1 ) % this.k;
        if( x3 < 0 ) {
            x3 += this.k;
        }
        if( y3 < 0 ) {
            y3 += this.k;
        }
        return [ x3, y3 ];
    };
```

Далі наведено код функції *ScalarMultiplication()*, яка реалізує демонстрацію процесу формування спільного секретного ключа:

```
$.ec.modk.ScalarMultiplication.prototype.getSubgroupOrder = function() {
        if( this.singular || !this.prime ) {
            return 0;
        }
        var n = 2;
        var q = this.addPoints( this.p, this.p );
        while( q !== null ) {
            q = this.addPoints( this.p, q );
            n += 1;
        }
        return n;
    };
```

Сама функція *ScalarMultiplication()* викликається у екземплярі життєвого циклу компоненту *mounted()*, як у наведеному нижче лістингу:

```
mounted() {
    $(function() {
      $.ec.curve = new $.ec.modk.ScalarMultiplication();
    });
  }
```

Стійкість системи у разі перехоплення проміжних результатів $Q(A)$ і $Q(\mathrm{B})$, які передаються відкритим каналом зв'язку, ґрунтується на складності розв'язання аналогу задачі дискретного логарифмування в групі точок еліптичних кривих.

Висновки та перспективи подальших пошуків у напрямі дослідження. Розроблений додаток є інтерактивним і дозволяє візуалізувати процеси виконання операцій додавання і множення, визначених для точок еліптичних кривих над полями дійсних чисел і Галуа, а також – продемонструвати використання цього апарату при формуванні спільного секретного ключа за протоколом Діффі-Хелмана, що значно спрощує розуміння цих процесів під час вивчення відповідних тем.

З метою запобігання відомим атакам, Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) рекомендує для використання п'ятнадцять еліптичних кривих різного рівня безпеки [5]. Таким чином, в подальшому розроблений додаток може бути розширеним за рахунок добавлення сторінок, які демонструють проблеми практичного впровадження криптографії на еліптичних кривих та способи їх вирішення.

Список літератури

1. ДСТУ 9041:2020. Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. (2020). Retrieved from: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=90523.

2. Stebila, D., Green, J. (2009). Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer. Network Working Group. Retrieved May 12, 2021, from https://tools.ietf.org/html/rfc5656.
3. Moeller, B., & Bolyard, & N., Gupta, & V., Blake-Wilson, S., & Hawk, C. (2006). Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). Retrieved May 12, 2021, from https://tools.ietf.org/html/rfc4492.
4. Jivsov, A. (2012). Elliptic Curve Cryptography (ECC) in OpenPGP. Retrieved May 12, 2021, from https://tools.ietf.org/html/rfc6637.
5. National Institute of Standards and Technology. (2013). FIPS 186-4. Digital Signature Standard (DSS). Retrieved from https://csrc.nist.gov/publications/detail/fips/186/4/final.
6. Standards for Efficient Cryptography/ (2009). SEC 1: Elliptic Curve Cryptography. Certicom Research. May 21, 2009 Version 2.0. Retrieved from https://www.secg.org/sec1-v2.pdf.