**11. Дайте загальну оцінку ЕЦП ДСТУ 4145 2002, порівняйте його з EC DSA по критеріям стійкість - складність?**

Національний стандарт ДСТУ 4145 – 2002 визначає механізм електронного цифрового підпису, він ґрунтується, як і ЕЦП згідно ISO/IEC 14888 – 3(15946 – 2), на властивостях груп точок еліптичних кривих над полями GF(2m). Цифровий підпис забезпечує автентичність повідомлення та неспростовність застосування особистого ключа, тобто автентифікацію власника цифрового підпису. При його застосуванні з необхідною ймовірністю гарантується цілісність підписаного повідомлення, автентичність його автора та неспростовність підписаного документу. У стандарті для генерування випадкових послідовностей використовуються міждержавний стандарт ГОСТ 28147 – 89 та ГОСТ 34.311 – 94 – для обчислення геш – функції повідомлення, що підписується.

В стандарті для тримання випадкових даних, необхідних для побудови загальних параметрів цифрового підпису, обчислення цифрового підпису, а також для побудови відкритих і особистих ключів цифровою підпису використовується генератор псевдовипадкових послідовностей. По суті він ґрунтується на стандарті ANSI США Х9. 17. допускається використання будь – якого іншого генератора, який рекомендований уповноваженим виконавчим органом державної влади.

Обов’язковою складовою ЕЦП національного стандарту є функція гешування H. Вона, як і в інших стандартах, застосовується в процесі обчислення й перевірки цифрового підпису.

Функція гешування Н перетворює інформацію М довільної довжини  на двійковий рядок Н(М) фіксованої довжини . Повинна використовуватися функція гешування, що визначена в ГОСТ 34.311 – 95 або будь-яка інша функція гешування, яка рекомендована уповноваженим виконавчим органом державної влади. Значення параметра довжини геш – значення  однозначно визначається ідентифікатором iH конкретної функції гешування, яка використовується сумісно з національним стандартом ЕЦП, він відноситься до загальних параметрів ЕЦП. Значення iH=1, L(iH)=8 відповідають функції гешування, що визначена в ГОСТ 34.311 - 93.

Схема цифрового підпису EC-DSA є аналогом схеми цифрового підпису DSA на еліптичних кривих. Схема є прикладом механізму вироблення цифрового підпису з додатком. Для застосування ЕЦП повинні бути заданими параметри домену та параметри користувачів. Бітова довжина модуля  повинна бути більше ніж бітова довжина вихідного значення геш - функції . Особистий й відкритий ключі об’єкта А,  і  відповідно, необхідно виробляти у відповідності із процедурою, що визначена у стандарті ISO/IEC 15946-1 та описана в п .

Вироблення цифрового підпису

Вхідними даними для процесу цифрового підпису[[1]](#footnote-1)) є наступні:

- параметри домену;

- особистий ключ  підписувача;

- повідомлення .

Вихідними даними процесу вироблення цифрового підпису є пара , що є цифровим підписом повідомлення  об’єкта A.

При підписуванні повідомлення  об’єкт A виконує такі кроки:

1. Обчислення геш - значення .
2. Вибір або генерування ключа сеансу - випадкового цілого числа , що належить діапазону .
3. Обчислення точки еліптичної кривої .
4. Обчислення відкритого к5люча сеансу .
5. Обчислення значення  в полі .
6. Обчислення значення цифрового то підпису.

Якщо у процесі обчислення цифрового підпису  або , тоді процес вироблення цифрового підпису необхідно повторити з новим випадковим значенням . (Але необхідно зазначити, що ймовірність того, що  або  є надзвичайно малою, якщо  обрано випадково та згідно вимог, що наведені в п .

Крім того, у зв’язку з тим, що обчислене значення  не залежить від повідомлення, що підписується, конфіденційний ключ сеансу, тобто число  та відкритий ключ сеансу – число , можуть обчислюватися попередньо, і надалі зберігатися та використовуватися під час вироблення цифрового підпису. Але відносно число  повинно зберігатись в таємниці, так як його компрометація може призвести до компрометації особистого ключа .

Таким чином, пара цілих чисел  становить цифровий підпис повідомлення  об’єкта А.

Перевіряння цифрового підпису

Перевіряння цифрового підпису здійснюється за 4 кроки:

- перевіряння розміру цифрового підпису;

- обчислення геш - значення повідомлення;

- обчислення на еліптичних кривих та перевіряння цифрового підпису.

Вхідними даними для перевіряння цифрового підпису є наступні:

- параметри домену;

- відкритий ключ  об’єкта А;

- підписане повідомлення , ;

- цифровий підпис повідомлення , що представлений двома цілими числами  та .

Для перевіряння цифрового підпису повідомлення  об’єкта , об’єктом В виконуються такі кроки.

1. Перевіряння того, що  та . Якщо хоч одна умова не виконуються, то цифровий підпис відхиляється.
2. Обчислення геш - значення  за допомогою геш - функції .
3. Обчислення оберненого в полі F(n) відносно  елемента .
4. Обчислення допоміжних даних  та .
5. Обчислення точки еліптичної кривої .
6. Обчислення .F

Якщо , тоді цифровий підпис повинен прийматися перевірником. Якщо , тоді цифровий підпис повинен відхилятися перевірником.

Особистий й відкритий ключі об’єкта А,  і  відповідно, необхідно виробляти у відповідності із вимогами, що визначені у стандарті ISO/IEC 15946-1 та наведені в п.

|  |  |  |  |
| --- | --- | --- | --- |
| Процес | Операція | ECDSA | ДСТУ 4145-2002 |
| Вироблення цифрового підпису |  | 1 | 1 |
|  | 1 | 1 |
|  | 1 | 0 |
| Множення в | 2 | 2 |
| Додавання (або віднімання) в | 1 | 1 |
| Скалярне множення точки кривої | 1 | 1 |
| Перевіряння цифрового підпису |  | 1 | 1 |
|  | 1 | 0 |
|  | 1 | 0 |
| Множення в | 2 | 1 |
| Скалярне множення точки кривої | 2 | 2 |
| Додавання точок на кривій | 1 | 1 |

**12. Які основні задачі криптоаналізу відносно DSA перетворення та при яких вхідних даних вони можуть вирішуватись? Що повинна відображати модель крипто аналітика та які його практичні та потенційні можливості відносно DSA перетворення ?**

У випадку, коли для формування елементів буде застосовуватись двохмодульне перетворення згідно DSA[60] або ГОСТ Р 34.10–94 (ДСТУ ГОСТ 34.310–2009, ГОСТ 34.310–95 [57]), то період повторення буде дорівнювати , оскільки показник степені може приймати значення не більше чим . Правило формування можна представити у вигляді

|  |  |  |
| --- | --- | --- |
|  | , . | (5.33 4.3) |

Із (5.33 4.3) слідує, що в цьому випадку формується підгрупа порядку . В DSA допустимим значенням є , а в ГОСТ Р 34.10–94 – . Наближено це буде відповідно дорівнювати  та .

Таким чином, при використанні в якості джерела первинної випадковості елементів полів або підгруп полів Галуа, забезпечується необхідний період повторення, а елементи поля чи підгрупи поля на періоді не повторюються. Вказана властивість, на наш погляд, дозволяє будувати ДГВБ з використанням елементів полів чи підгруп полів.

Також замітимо, що з точки зору оперативності проходження експертизи алгоритму генерування елементів поля та побудови ДГВБ, краще застосовувати методи, для яких уже розроблені та атестовані методи генерування загальних параметрів, наприклад, що містяться в DSA [60] або ГОСТ Р 34.310–95 [57]. Детально деякі необхідні теоретичні оцінки викладених вище питань розглядаються в 6 розділі.

**13. В чому сутність атаки на ЕЦП в групі точок ЕС з використанням зв’язаних ключів та як забезпечити захист від неї?**

У цій моделі атакуючий може спостерігати результати процесу зашифрування / розшифрування на різних секретних ключах. Атакуючий знає (або навіть сам здатний вибирати) співвідношення між різними ключами, але не знає самих ключів. Наприклад, співвідношення може бути просто значенням за модулем з відомою константою: KB=KAmod C або більш складний зв'язок виду KB= F(KA), де F – довільна функція, вибрана.

Сутність атаки полягає в тому, що:

1. Криптоаналітику відомо 2**n**/2 пар (**P**, **C**) відкритих текстів та відповідних їм шифр текстів (зашифрованих на ключі **K**), де **n** – розмір блоку даних в бітах, що шифруються.

2. Криптоаналітику відомо стільки ж (2**n**/2) пар текстів (**P’**, **C’**), отриманих вже з використанням ключа **K’**, зв’язаного з **K**.

Для кожного співвідношення текстів (**P**, **C**) та (**P’**, **C’**) криптоаналітик розв’язує систему рівнянь:

**F(P, k\*) = P’,**

**F(C, k\*) = C’.**

Криптоаналітик не може знати наперед, який з 2**n/2** текстів **P’** відповідає конкретному тексту **P**. Проте вірогідність того, що 2 випадкових тексти будуть відповідати необхідному відношенню, дорівнює 2**-n**; відповідно, необхідна пара (**P**, **P’**) повинна бути знайдена в середньому після аналізу не більш, ніж 2**n**/**2 + 1** текстів.

Досить імовірно, що якийсь ключ **k\***, що задовольняє наведеним вище рівнянням, і є шуканий підключ **k1**. В залежності від процедури розширення ключа знання **k1** може дати криптоаналітику достатньо багато інформації щодо ключа **K**.

Необхідна умова для проведення даної атаки полягає в тому, що функція раунду F() алгоритму, що атакується, повинна бути досить слабкою для обчислення k \*, що, однак, можна сказати стосовно більшості сучасних алгоритмів шифрування.

Залежно від структури самого алгоритму шифрування, трудомісткість атаки може бути істотно менше описаного вище загального випадку.

Описана атака на зв'язаних ключах не виглядає практичною. Легко погодитися з тим, що вона вимагає занадто великої кількості припущень. Дана атака досить довго вважалася досить потужною, але суто теоретичною. Однак, зараз багато експертів вважають, що атаки на пов'язаних ключах можуть мати практичне застосування. Зазначимо, що основна умова для атаки виглядає досить дивно: криптоаналитик може писати ключ (тобто модифікувати шуканий невідомий ключ потрібним чином), але не може його читати. Тим не менш, деякі реалізації криптоалгоритмів або мережевих протоколів (наприклад, протоколів аутентифікації або обміну ключами) можуть бути атаковані з використанням пов'язаних ключів.

Відносно ЦП EC-DSA показано, що якщо особисті ключі сеансу зв’язані будь яким чином (відомим зловмиснику, тобто відбувається атака на зв'язаний ключах, наприклад k1+k2=n,n – порядок базової точки), то перші складові підпису r1=r2 в деяких повідомленнях Mi, Mj будуть однаковими. Якщо особистий ключ формується за правилом , де h1 та h2 є геш-значення для повідомлень Мі та Мj, то для повідомлень Мі та Мj будуть вироблені одинакові ЦП. Таким чином атака може бути реалізована тільки для двох наперед заданих повідомлень. При цьому порушник може виготовити для свого повідомлення такий самий ЦП. Таким чином, використання функції вирізання тільки х-координати при обчислення відкритого параметру сеансу ЦП робить стандарт EC DSA уразливим як щодо можливості створення колізій ЦП, так і визначення особистого ключа. Цікаво, що при цьому ключ порушника так само компрометується і він буде змушений його змінити після появи таких повідомлень.

Розглянемо вироблення підпису при EC-KCDSA

|  |  |
| --- | --- |
| Для повідомлення Мі | Для повідомлення Мj |
| 1.  2.  3.  4.  5.  6.  7. | 1.  2.  3.  4.  5.  6.  7. |

Визначимо умови, за яких -компоненти ЦП EC KCDSA співпадають, тобто  для двох довільних різних повідомлень Мі та Мj. Використовуючи значення сьомих рядків, маємо:  абоДалі отримаємо, що:

або



Тобто щодо EC-KCDSA при таких умовах значення відкритих ключів r1 та r2 не співпадають, тобто колізія не відбувається (це видно з третього і п’ятого рядків). Більше того, здійснення атаки на зв’язаних ключах носить експоненційний характер і практично неможлива.

Таким чином, із алгоритмів стандарту ЦП ISO/IEC 15946-2 алгоритм EC-DSA вразливий до атаки на зв’язаних ключах, а EC-KCDSA – захищений.

**14. В чому сутність атаки на програмну реалізацію ЕЦП ECDSA та як забезпечити захист від неї?**

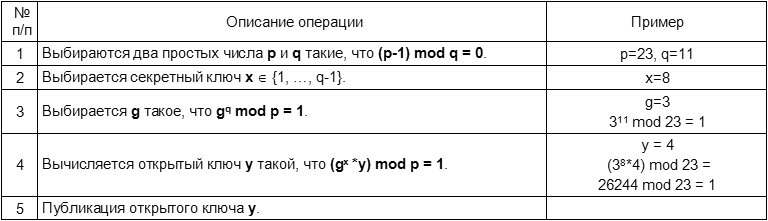
В алгоритмах, що базуються на еліптичних кривих (в тому числі і в розглянутому ECDSA алгоритмі) використовуються два типи операцій - додавання чисел на еліптичній кривій і подвоєння числа. Допускаючи, що пристрій, що виконує обчислювальні операції при створенні електронного цифрового підпису за стандартом ECDSA, підключено до незахищеного джерела живлення, до якого має доступ зловмисник, недоброзичливець може отримати осцилограму споживання потужності даними устройством.Допуская, що модуль еліптичної кривої відомий, відомо підписується повідомлення, і в межах одного повідомлення використовується один і той же секретний ключ, грунтуючись на отриманих з осцилограми даних і використовуючи відомий алгоритм [2], можна відновити приватний ключ.

Існує кілька методів протидії такого роду атак, але, як правило, контрзаходи включають в себе навмисні зміни в алгоритмах - впровадження додаткових «порожніх» операцій.

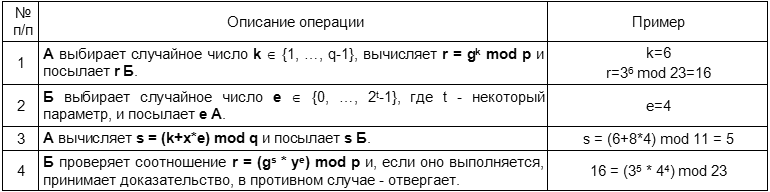
Ефективність контрзаходів в значній мірі залежить від характеристик апаратної платформи, операційного середовища, можливостей противника і повинна оцінюватися на основі кожного конкретного випадку.

**15. В чому сутність криптографічного протоколу Шнора та які його властивості?**

Этап 1. Генерація ключів



Этап 2. Аутентификация.



Для забезпечення стійкості протоколу в 1989 р Шнорр рекомендував використовувати p довжиною 512 біт, q довжиною 140 біт і t = 52.

**16. Дайте загальну оцінку ЕЦП ДСТУ 4145 - 2002, порівняйте його з ЕЦП ГОСТ 34.10 – 2012?** Стандарт України ДСТУ 4145-2002[52] визначає механізм електронного цифрового підпису, що ґрунтується на властивостях груп точок еліптичних кривих над полями GF(2m). Цифровий підпис забезпечує автентичність повідомлення та неспростовність застосування особистого ключа, тобто автентифікацію власника цифрового підпису. При його застосуванні з необхідною ймовірністю гарантується цілісність підписаного повідомлення, автентичність його автора та неспростовність підписаного документа. У стандарті для генерування псевдовипадкових послідовностей використовуються міждержавний стандарт ГОСТ28147-89[55],та ГОСТ34.311-94[58] – для обчисленнягеш-функціїповідомлення, що підписується. Детальний повний опис стандарту міститься у [58].

У стандарті для отримання випадкових даних, необхідних для побудови загальних параметрів цифрового підпису, обчислення цифрового підпису, а також для побудови відкритих і особистих ключів цифрового підпису використовується генератор псевдовипадкових послідовностей. По суті, він ґрунтується на стандарті ANSI США Х9.17 [312]. Допускається використання будь-якогоіншого генератора, рекомендованого уповноваженим виконавчим органом державної влади.

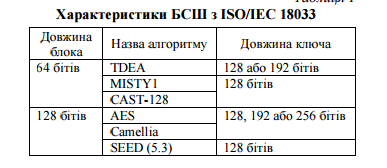
Обов’язковою складовою ЦП національного стандарту є функція гешування *H*. Вона, як і в інших стандартах, застосовується в процесі обчислення й перевірки цифрового підпису.

Функція гешування *Н*перетворює інформацію*М*довільної довжини*LT*на двійковий

рядок Н(М) фіксованої довжини *LH*. Повинна використовуватися функція гешування, визначена в ГОСТ34.311-95абобудь-якаінша функція гешування, рекомендована уповноваженим виконавчим органом державної влади. Значення параметра довжини геш-

значення *LH*однозначно визначається ідентифікатором iH конкретної функції гешування, що використовується сумісно з національним стандартом ЦП. Ідентифікатор iH належить до загальних параметрів ЦП. Значення iH = 1, L(iH) = 8 відповідають функції гешування, що визначена в ГОСТ34.311-96.

**17. Обґрунтуйте та виберіть параметри БСШ та оцініть його криптографічну стійкість?**

****

Проведений аналіз спеціальних вимог, які визначають певні параметри криптографічного перетворення, дав змогу сформулювати такі обмеження та вимоги до перспективного БСШ.

1. Захищеність алгоритму від криптоаналітичних атак. Основними методами криптографіч- ного аналізу є: диференціальний криптоаналіз, розширення для диференціального криптоаналізу, пошук найкращої диференціальної характеристики, лінійний криптоаналіз; інтерполяційне вторгнення; вторгнення із частковим угадуванням ключа; вторгнення з використанням зв'язаного ключа; вторгнення на основі обробки збоїв; пошук лазівок та потенційні атаки тощо.

2. Статистична безпека криптографічного алгоритму в плані нерозрізнюваності гам шифрування та шифротекстів від істинно випадкових [9].

3. Особливості конструкції та відкритість структури. Криптоалгоритм повинен мати зрозумілу, легку для аналізу структуру й ґрунтуватися на надійному математичному апараті.

4. Стійкість до модифікації, коли всіх кандидатів перевіряють на стійкість до різноманітних модифікацій: стійкість до криптоаналітичних атак у разі зменшення кількості циклів, скорочення компонентів, використовуваних алгоритмом тощо.

5. Обчислювальна складність (швидкість) за шифрування/розшифрування. Складність програмної, апаратної й програмно-апаратної реалізації повинна оцінюватися обсягом пам'яті як для програмної, так і для апаратної реалізації, зокрема за програмної реалізації – кількістю необхідної оперативної пам'яті, розміром вихідного коду, швидкістю роботи програми на різних платформах за реалізації на відомих мовах програмування. За апаратної оцінюється кількістю вентилів і швидкістю в Мб/с.

6. Універсальність криптографічного алгоритму: можливість роботи з різними довжинами початкових ключів та інформаційних блоків; безпека реалізації на різних платформах і додатках; можливість використання криптографічного алгоритму в необхідних обґрунтованих режимах роботи БСШ.

7. Загальні вимоги до БСШ повинен визначати замовник у вигляді конкретних параметрів криптоалгоритму.

Оцінюючи криптографічну стійкість, необхідно враховувати, що деяка модифікація або доповнення алгоритму виконання криптоаналізу можуть істотно змінити складність проведення атаки. Так, використання 2R-атаки в диференційному криптоаналізі DES дало змогу зменшити складність і зробити цю атаку ефективнішою, ніж пряме перебирання ключів. Тому, оцінюючи ефективність методу криптоаналізу, необхідно враховувати такі фактори:

−рівень доступності відкритих повідомлень для криптоаналітика;

−умови проведення атаки – можливість вибору значень на входах шифратора і/або залежностей між ними; −перелік алгоритмів, відносно яких може бути застосований метод криптоаналізу;

−можливості вибору криптоаналітиком значень відкритих повідомлень;

−можливість та необхідність наявності у криптоаналітика фізичного доступу до обладнання;

−мінімальна складність виконання проведення атаки на повний шифр;

−універсальність методу криптоаналізу, тобто можливість його застосування до поширених шифрів.

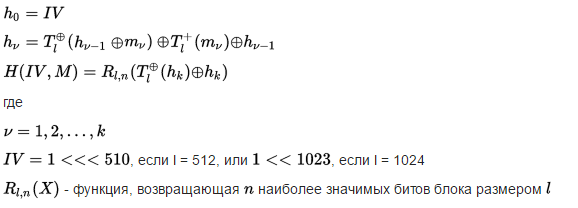
Також необхідно враховувати, що універсальність, мінімальні вимоги до умов проведення атаки й низька складність збільшують ефективність методу криптоаналізу. Своєю чергою, необхідність наявності відкритих текстів, їх вибору або завдання залежності між секретними ключами знижує ефективність. Також вимога наявності фізичного доступу до обладнання істотно звужує спектр застосування методу криптоаналізу і, відповідно, також знижує його ефективність.

**18. Дайте загальну оцінку ФГ ДСТУ 7564 - 2014,та порівняйте її з ФГ ДСТУ ГОСТ 34.311 – 2009?**

Kupyna - ітеративна криптографічний хеш-функція. Прийнята в якості національного стандарту України ДСТУ 7564: 2014 в якості заміни застарілої хеш-функції ГОСТ 34.311-95. Стискаюча функція Kupyna складається з двох фіксованих 2n-бітних перестановок T⊕ і T +, структура яких запозичена у шифру Kalyna. Зокрема, використовується чотири таких же S-блоки. Результат роботи хеш-функції може мати довжину від 8 до 512 біт. Варіант, який повертає n біт, називається Kupyna-n.

Спочатку повідомлення М доповнюється до довжини, кратної розміром блоку. Для цього до повідомлення додається 1 біт, потім d нульових бітів, де d=(-N – 97) mod 1 і 96 біт, що містять довжину повідомлення в бітах. Таким чином, максимальна довжина повідомлення 296 -1 бітів.

Після цього повідомлення разбивається на t блоків m1,m2,…,mt по t бітів кожний. Для варіантів функції, повертаючих до 256 біт, l = 152. Для варіантів, повертаючих більші значення, l=1024. Далі будується хеш-функція, використовуючи наступний ітеративний алгоритм:



**19. В чому сутність атак груба сила відносно БСШ та оцініть їх застосування?**

При проведении криптоанализа схем поточного шифрования подразумевается, что атака может быть успешно   
реализована, если ее вычислительная сложность меньше, чем вычислительная сложность полного перебора всего   
пространства ключей шифра. Анализ показывает, что к рассматриваемым схемам поточного шифрования   
наибольшую вероятность применения имеют следующие атаки [12]:   
1. Атака грубой силы или исчерпывающий поиск ключа (Exhaustive key search). Теоретически, данный вид атаки   
должен быть наиболее эффективным по сравнению с остальными атаками. При реализации этой атаки   
осуществляется полный перебор всех возможных ключей. Считается, что у стойких шифров сложность любой   
аналитической атаки должна быть не меньше сложности атаки “грубая сила”.

DES, как первый блочный шифр, имеющий важное значение, прошел через много испытаний на безопасность. Среди предпринятых атак лишь три представляют интерес: грубая сила, дифференциальный криптоанализ и линейный криптоанализ.   
  
Атака грубой силы   
Мы уже обсуждали слабость шифра с коротким ключом. Слабость ключа совместно с другими рассмотренными недостатками, делает очевидным, что DES может быть взломан с числом испытаний 255. Однако сегодня большинство приложений использует либо 3DES с двумя ключами (размер ключа 2112 ), либо 3DES с тремя ключами (размер ключа 2168 ). Эти две многократных версии DES позволяют ему показывать существенную стойкость к атакам грубой силы.

**20. Дайте загальну оцінку ЕЦП ДСТУ 4145 2002, порівняйте її з EC DSA по стійкості та швидкодії?**

Національний стандарт ДСТУ 4145 – 2002 визначає механізм електронного цифрового підпису, він ґрунтується, як і ЕЦП згідно ISO/IEC 14888 – 3(15946 – 2), на властивостях груп точок еліптичних кривих над полями GF(2m). Цифровий підпис забезпечує автентичність повідомлення та неспростовність застосування особистого ключа, тобто автентифікацію власника цифрового підпису. При його застосуванні з необхідною ймовірністю гарантується цілісність підписаного повідомлення, автентичність його автора та неспростовність підписаного документу. У стандарті для генерування випадкових послідовностей використовуються міждержавний стандарт ГОСТ 28147 – 89 та ГОСТ 34.311 – 94 – для обчислення геш – функції повідомлення, що підписується.

В стандарті для тримання випадкових даних, необхідних для побудови загальних параметрів цифрового підпису, обчислення цифрового підпису, а також для побудови відкритих і особистих ключів цифровою підпису використовується генератор псевдовипадкових послідовностей. По суті він ґрунтується на стандарті ANSI США Х9. 17. допускається використання будь – якого іншого генератора, який рекомендований уповноваженим виконавчим органом державної влади.

Обов’язковою складовою ЕЦП національного стандарту є функція гешування H. Вона, як і в інших стандартах, застосовується в процесі обчислення й перевірки цифрового підпису.

Функція гешування Н перетворює інформацію М довільної довжини  на двійковий рядок Н(М) фіксованої довжини . Повинна використовуватися функція гешування, що визначена в ГОСТ 34.311 – 95 або будь-яка інша функція гешування, яка рекомендована уповноваженим виконавчим органом державної влади. Значення параметра довжини геш – значення  однозначно визначається ідентифікатором iH конкретної функції гешування, яка використовується сумісно з національним стандартом ЕЦП, він відноситься до загальних параметрів ЕЦП. Значення iH=1, L(iH)=8 відповідають функції гешування, що визначена в ГОСТ 34.311 - 93.

Схема цифрового підпису EC-DSA є аналогом схеми цифрового підпису DSA на еліптичних кривих. Схема є прикладом механізму вироблення цифрового підпису з додатком. Для застосування ЕЦП повинні бути заданими параметри домену та параметри користувачів. Бітова довжина модуля  повинна бути більше ніж бітова довжина вихідного значення геш - функції . Особистий й відкритий ключі об’єкта А,  і  відповідно, необхідно виробляти у відповідності із процедурою, що визначена у стандарті ISO/IEC 15946-1 та описана в п .

Вироблення цифрового підпису

Вхідними даними для процесу цифрового підпису[[2]](#footnote-2)) є наступні:

- параметри домену;

- особистий ключ  підписувача;

- повідомлення .

Вихідними даними процесу вироблення цифрового підпису є пара , що є цифровим підписом повідомлення  об’єкта A.

При підписуванні повідомлення  об’єкт A виконує такі кроки:

1. Обчислення геш - значення .
2. Вибір або генерування ключа сеансу - випадкового цілого числа , що належить діапазону .
3. Обчислення точки еліптичної кривої .
4. Обчислення відкритого к5люча сеансу .
5. Обчислення значення  в полі .
6. Обчислення значення цифрового то підпису.

Якщо у процесі обчислення цифрового підпису  або , тоді процес вироблення цифрового підпису необхідно повторити з новим випадковим значенням . (Але необхідно зазначити, що ймовірність того, що  або  є надзвичайно малою, якщо  обрано випадково та згідно вимог, що наведені в п .

Крім того, у зв’язку з тим, що обчислене значення  не залежить від повідомлення, що підписується, конфіденційний ключ сеансу, тобто число  та відкритий ключ сеансу – число , можуть обчислюватися попередньо, і надалі зберігатися та використовуватися під час вироблення цифрового підпису. Але відносно число  повинно зберігатись в таємниці, так як його компрометація може призвести до компрометації особистого ключа .

Таким чином, пара цілих чисел  становить цифровий підпис повідомлення  об’єкта А.

Перевіряння цифрового підпису

Перевіряння цифрового підпису здійснюється за 4 кроки:

- перевіряння розміру цифрового підпису;

- обчислення геш - значення повідомлення;

- обчислення на еліптичних кривих та перевіряння цифрового підпису.

Вхідними даними для перевіряння цифрового підпису є наступні:

- параметри домену;

- відкритий ключ  об’єкта А;

- підписане повідомлення , ;

- цифровий підпис повідомлення , що представлений двома цілими числами  та .

Для перевіряння цифрового підпису повідомлення  об’єкта , об’єктом В виконуються такі кроки.

1. Перевіряння того, що  та . Якщо хоч одна умова не виконуються, то цифровий підпис відхиляється.
2. Обчислення геш - значення  за допомогою геш - функції .
3. Обчислення оберненого в полі F(n) відносно  елемента .
4. Обчислення допоміжних даних  та .
5. Обчислення точки еліптичної кривої .
6. Обчислення .F

Якщо , тоді цифровий підпис повинен прийматися перевірником. Якщо , тоді цифровий підпис повинен відхилятися перевірником.

Особистий й відкритий ключі об’єкта А,  і  відповідно, необхідно виробляти у відповідності із вимогами, що визначені у стандарті ISO/IEC 15946-1 та наведені в п.

|  |  |  |  |
| --- | --- | --- | --- |
| Процес | Операція | ECDSA | ДСТУ 4145-2002 |
| Вироблення цифрового підпису |  | 1 | 1 |
|  | 1 | 1 |
|  | 1 | 0 |
| Множення в | 2 | 2 |
| Додавання (або віднімання) в | 1 | 1 |
| Скалярне множення точки кривої | 1 | 1 |
| Перевіряння цифрового підпису |  | 1 | 1 |
|  | 1 | 0 |
|  | 1 | 0 |
| Множення в | 2 | 1 |
| Скалярне множення точки кривої | 2 | 2 |
| Додавання точок на кривій | 1 | 1 |

1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)