3-4. Призначення та сутність стандарту ДСТУ ISO/IEC 15946 - 1 та який порядок його застосування.?

**4. Назвіть та дайте характеристику загальних параметрів еліптичних кривих, які можуть застосовуватись в криптографії для ЕЦП?**

До загальних параметрів еліптичної кривої *Е*над полем  належать такі параметри:

1. Розмір поля , який визначає базове кінцеве поле , де  повинно бути простим числом.
2. Бітовий рядок , якщо еліптична крива генерована випадково. У [22] наведено приклад того, як генерувати випадкову еліптичну криву та контролювати її параметри, використовуючи для ініціалізації рядок  (необов’язково).
3. Параметри  та  еліптичної кривої, які визначають рівняння еліптичної кривої , що використовується: .
4. Базова точка  порядку  з координатами  та.
5. Порядок  базової точки  за умови, що  та  – просте число.
6. Кофактор  взаємозв’язку порядку кривої  та порядку базової точки , причому .
7. Крива, тобто її параметри 1–6, ні в якому разі не повинні вибиратись із переліку значень, що виключені зі списку (не рекомендуються або заборонені).

Проведений аналіз дозволив сформулювати вимоги до розміру та властивостей загальних параметрів еліптичних кривих. Сутність цих вимог викладена нижче.

Порядок кривої порядок базової точки  еліптичної кривої та модуль перетворення  взаємопов’язані:  

 

В цілому маємо:

 



Співвідношення дозволяють вибрати вказані загальні параметри ЕК.

Параметри еліптичної кривої над *F(q),* включаючи особливі випадки *F(p)* і *F*(2*m*), мають визначати:

– розмір поля *q* = *pm*,який визначає базове скінченне поле *F(q)*, де *p* має бути простим числом, і вказує на базис, що використовується для представлення елементів поля у разі *m >*1;

– якщо *q* = *pm, причому* *p* > 3, два елементи поля *a* і *b* у *F*(*q*), які визначають рівняння еліптичної кривої:

*E*: *y*2 = *x*3+ *ax*+ *b*;

⎯ якщо *q* = 2*m*, то два елементи поля *a* і *b* у *F*(2*m*), які визначають рівняння еліптичної кривої:

*E*: *y*2 *+ xy = x*3 *+ ax*2 *+ b*;

⎯ якщо *q* = 3*m*, то два елементи поля *a* і *b* у *F*(3*m*), які визначають рівняння еліптичної кривої:

*E*: *y*2 *= x*3 *+ ax*2 *+ b*;

⎯ елементи поля *xG* і *yG* у *F*(*q*), які визначають базову точку *G = (xG*, *yG)* порядку *n* на еліптичній кривій *E*;

⎯ порядок *n* базової точки *G*;

⎯ значення кофактора *h* = *#E(F(q))*/*n,* якщо воно вимагається базовою схемою криптографічного перетворення.

* Порядок кривої: Еліптична крива *E* над полем *F(q)* має бінарною операцією «+» складання точок *E* × *E* → *E,* для якоїдвом точкам *Q*1, *Q*2на *E* може бути обчисленатретя точка *Q1* + *Q2* на *E.* Еліптична крива *E* є абелевою групою щодо операції «+».

Число точок еліптичної кривої *E* (включаючи точку нескінченності 0*E*) називається порядком *E* і позначається як *#E(F(q)).* Порядок кривої *#E(F(q))* визначається згідно з теоремою Хасе

Еліптичні криві можуть бути побудовані над полями *GF*(*p*), *GF*(2*m*) та *GF*(*pm*).

Параметрами ЕК є числа або поліноми *а* та *b*, а також базова точка *G* та її порядок *n*.

Порядок еліптичної кривої зв’язаний з порядком базової точки, як , де .

Усі методи побудови простих чисел можна розділити на 3 класи [22]:

* аналітичні, що дозволяють побудувати строго прості числа;
* "псевдопрості", що дозволяють побудувати псевдопрості числа;
* числа, що будуються на основі гіпотез (не доведених).

Найбільше розповсюдження знайшов тест Рабінера-Міллера побудови псевдовипадкових чисел [10]. Нехай *m* – непарне, що перевіряється на простоту. Подамо *m*-1 у вигляді:

. (1.97)

В подальшому знайдемо для випадкового цілого *а*

. (1.98)

З урахуванням (1.97) маємо, що:

. (1.99)

У ряді (1.98) кожний попередній елемент є коренем з наступного елемента.

Якщо , , то ряд (1.98) складається з одиниць, перед якими може з’являтися -1, при цьому

, (1.100)

для всіх 0 ≤ *j* ≤ *s* , чи .

Число *m*, що задовольняє хоча б одну умову, називається сильним псевдопростим у змісті Рабінера – Міллера.

Якщо проводити *t* іспитів, для різних випадкових *а*, то імовірність того, що в кожному іспиті не буде виявлене просте число, не перевищує ¼.

На *t* іспитах імовірність того, що число *Рс* є складене, визначається як

. (1.101)

Перевірка з використанням тесту Рабінера-Міллера здійснюється за алгоритмом:

1. ;
2. Якщо НСД  ≠1, *m* – складене;
3. ;
4. якщо , *m* – можливо просте;
5.  доти поки ;
6. якщо , то *m* – складене;

якщо , *m* – можливо просте.

5-6. Призначення та сутність стандарту ДСТУ ISO/IEC 15946 - 3 та який порядок його застосування.?

**6.Дайте визначення Галуа та які умови існування скінченного поля Галуа F(рm)? Дайте визначення та які основні властивості еліптичної криві над скінченним полем Галуа F(2m)?**

Для будь-якого позитивного цілого m і простого p існує скінченне поле Галуа з точно pm елементів. Це поле унікальне й визначається з точністю до ізоморфізму та називається скінченним полем F(pm).

Необхідно враховувати, що F(pm) – це загальне позначення, його частковими випадками є поле F(p) для m = 1 і поле F(2m) для p = 2. Якщо p = 2, то елементи поля можуть бути ідентифіковані за допомогою бітових рядків довжини m, і сума двох елементів поля визначається як побітове XOR (сума за модулем 2) двох бітових рядків.

Визначення скінченного поля F(pm). Для будь-яких простих  і додатного цілого числа  існує скінченне поле, що складається точно з  елементів. Це поле однозначно визначене з точністю до ізоморфізму та у цьому стандарті подане як скінченне поле .

Для елементів поля  визначено дві основні операції, додавання  та множення такі що: елементи поля  відносно операції додавання  є абелевою групою; елементи групи  відносно операції множення  є абелевою групою. Існує багато способів побудови скінченного поля з  елементів. Скінченне поле  може бути відображене як векторний простір розмірності  над полем . Тобто, існує  елементів  у полі  таких, що кожний елемент  може бути однозначно поданий у формі , де . Такий, набір  елементів називають базисом поля  над полем . При використанні такого базису елемент поля  може бути наведений у вигляді вектора . Такий елемент поля  позначають -арним рядком  довжини , тобто

.

Існує багато різних базисів  над полем . Відповідно для кожного базису можуть бути визначені множина елементів поля та операція множення.

Зазвичай, групу елементів  визначають як . Це циклічна група порядку . Отже, існує щонайменше один елемент  у полі  такий, що кожний елемент  у полі  може бути однозначно записаний як , для деякого .

Зворотній елемент групи . Нехай  буде елементом групи . Тоді існує єдиний  такий, що , і елемент  називається мультиплікативно зворотнім до елемента  (інверсією), позначається як , та може бути обчислений як .

Характеристика скінченного поля F(pm). Якщо для досягнення нульового елементу потрібно  додавань одиничного елементу, тоді  називають характеристикою поля. Якщо нульовий елемент не може бути досягнуто додаванням одиничних елементів, тоді  є нулем, а не нескінченним елементом.

Ділення в полі F(pm). Значення  у полі  існує, якщо знаменник не нульовий. У цьому випадку частка .

є квадратом у полі ,  .

Пошук квадратних коренів в полі F(pm). Для знаходження квадратних коренів у полі  існують різні методи. Їх застосування дозволяє для кожного  знайти  таке, що , де  є квадратом числа . Один з таких методів може бути одержаний простою модифікацією (замінити  замість ) методу для знаходження квадратних коренів у полі .

Визначення поля. Для будь-якого цілого числа  існує скінченне поле, яке складається точно з  елементів. Це поле є однозначним з точністю до ізоморфізму та розглядається як скінченне поле .

Скінченне поле  може бути ототожнено з набором бітових рядків довжини  таким чином. Кожне скінченне поле  має щонайменше один базис  такий, що кожний елемент  має однозначне подання у вигляді , де  для . Елемент  може потім бути ототожнений з бітовим рядком . Задача вибору базису виходить за межі сфери застосування цього стандарту. Для елементів поля  визначено дві операції додавання та множення для яких справедливі умови:

елементи поля  відносно операції додавання  є абелевою групою;

елементи групи  відносно операції множення  є абелевою групою. Зазвичай набір елементів  визначають як . Це циклічна група порядку . Отже, існує щонайменше один елемент  у полі  такий, що кожний елемент  у полі  може бути однозначно записаний як , для деякого .

Мультиплікативну одиницю цієї групи визначають як . Тобто для кожного елементу  виконується 

Зворотній елемент групи .Нехай  буде елементом групи . Тоді існує єдине  такий, що , і елемент  називається мультиплікативно зворотнім до елемента  (інверсією), позначається як , та може бути обчислений як .

Характеристика скінченного поля. Якщо для досягнення нульового елементу потрібно  додавань одиничного елементу, тоді  називають характеристикою поля. Якщо нульовий елемент не може бути досягнуто додаванням одиничних елементів, тоді  є нулем, а не нескінченним елементом.

Ділення в полі . Значення  у полі  існує, якщо знаменник не нульовий. У цьому випадку частка .

Скінчені поля, що використовуються, у цьому розділі розглядають як упорядкований набір елементів. Інакше відображення крива – точки несуперечливим чином буде неможливим.

**7. Дайте класифікацію існуючих ЕЦП з додатком? Порівняйте ЕЦП в скінченному полі та групі точок ЕС ?**

Основним недоліком симетричних криптоперетворень є те, що з їх використанням не можна реалізувати модель взаємної недовіри.

Використання систем з відкритими ключами (перетворення в полях, кільцях та групах точок ЕК) дозволяє реалізувати модель взаємної недовіри та взаємного захисту.

Підпис, у тому числі і електронний цифровий, має володіти такими властивостями:

* автентичність підпису;
* мала ймовірність підробки підпису під документом;
* мала ймовірність не виявлення зміни змісту документа;
* неможливість “приклеювання” до нового документа підпису зі старого документа;
* незаперечність підпису;
* упізнавання підпису тощо.

Поняття електронного цифрового підпису (ЕЦП).Під ЕЦП розуміється деякий числовий еквівалент звичайного підпису (штампу, печатки і т.ін.), наявність яких дозволяє встановити цілісність та достовірность документа. Підробити цей підпис можна лише з ймовірністю, що не перевищує допустиму  . В [6] дано визначення електронного підпису (ЕП). ЕП – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації підписувача цих даних.

Під ЕЦП розуміється криптографічна контрольна сума, що обчислюється з використанням асиметричної криптографії. В [6] дано визначення ЕЦП. Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Під відкритим електронним підписом (ВЕП) розуміється сукупність відкритих даних, що характеризуються:

* інформацією, що захищається;
* взаємодією абонентів;
* часом створення та часом життя інформації та інше.

Таким чином відкритий підпис є сукупністю даних

,де  – зжате перетворення інформації (геш-функція),  – ідентифікатор відправника,  – час життя та створення,  – ідентифікатор отримувача,  – деякий параметр.

На основі ВЕП формується ЕЦП: ,

де  – дані користувачів,  – інформація,  – ключ прямого перетворення.

Вимоги до ЕП та ЕЦП:

1. складність обчислення ЕП та ЕЦП має бути не вища поліноміальної;
2. алгоритм обчислення криптоперетворення ЕЦП має бути загально-доступним;
3. складність знаходження  для ЕЦП має бути не нижча, ніж експоненціальна;
4. ЕЦП (ЕП) має бути дуже чутливим до зміни навіть одного біту в повідомленні, ключі та параметрах;
5. ЕЦП (ЕП) має дозволяти проводити перевірку цілісності та справжності повідомлення, тобто з високою ймовірністю знаходити порушення цілісності та справжності;
6. ЕЦП має бути захищеним від будь-якого класу криптоаналітичних атак (складність яких менше, ніж складність атаки “груба сила”) тощо.

Класифікація на основі криптоперетворення в полях, кільцях та групах точок еліптичних кривих. На теперішній час в частині додатків розроблений ЕЦП, який використовується в криптографічних протоколах для реалізації:

* безпечних електронних виборів;
* сумісний електронний підпис контрактів;
* груповий підпис з забезпеченням анонімності;
* довірений підпис;
* незаперечний підпис;
* сліпий підпис;
* підпис типу – передача, що забувається;
* виробка загального секрету тощо.

Наведена нижче класифікація дозволяє визначити властивості будь-якого відомого алгоритму цифрового підпису та зробити порівняння його з іншими алгоритмами, а також визначити за рядом критеріїв кращий із них. Стандартизовані та застосовуються цифрові підписи з додатком та цифрові підписи з відновленням повідомлення.

* Класифікація ЦП, на наш погляд, може бути здійснена за такими ознаками та критеріями .

1. За кількістю учасників:

* *Одиночний* – коли в процесі вироблення електронного цифрового підпису достатньо одного учасника;
* *Груповий* – коли в процесі вироблення цифрового підпису беруть участь більше ніж один учасник. При цьому груповий підпис може здійснюватись:

– із залученням для здійснення цифрового підпису послуги третьої довірчої сторони;

* без залучення третьої довірчої сторони.

1. За терміном дії ключів:

* Цифрові підписи без терміну обмеження дії ключів;
* Цифрові підписи з терміном обмеження дії ключів.

1. За способом перевірки:

* *Інтерактивні* – схеми цифрового підпису, що потребують протокольної взаємодії учасників. При цьому інтерактивні цифрові підписи можуть також бути незаперечними. Незаперечні цифрові підписи – це підписи, що не дають можливості перевірки цифрового підпису без дозволу суб’єкта (об’єкта), що підписує;
* *Неінтерактивні* – схеми цифрового підпису, що не потребують протокольної взаємодії учасників.

1. За способом вироблення підпису:

* *Цифровий підпис з відновленням* – частина або повне повідомлення може бути відновлене з цифрового підпису;
* *Цифровий підпис з додаванням* – цифровий підпис приєднується до повідомлення і в такому вигляді надсилається адресату;
* *Сліпий цифровий підпис* – цифровий підпис, що здійснюється без можливості перегляду змісту повідомлення;
* *Цифровий підпис за дорученням* – який здійснюється довірчим суб’єктом від імені суб’єкта, що довіряє, без надання довірчому суб’єкту таємних ключів суб’єкта, що довіряє;
* *Цифровий підпис контракту* – коли документ (контракт) підписується одночасно двома підписами (сторонами).

1. За потребою використання при виробленні цифрового підпису каналу зв’язку:

* Цифрові підписи з інтерактивним каналом зв’язку;
* Цифрові підписи з автономним каналом зв’язку.

1. Математична задача, на якій засновується стійкість цифрового підпису:

* Схеми цифрового підпису, стійкість яких заснована на складності задачі розкладання на співмножники великого числа – модуля перетворення;
* Схеми цифрового підпису, стійкість яких заснована на складності розв’язання задачі дискретного логарифму в полях Галуа;
* Схеми цифрового підпису, стійкість яких заснована на задачі дискретного логарифму в групі точок еліптичної кривої;
* Схеми цифрового підпису, стійкість яких заснована на складності розв’язання задачі дискретного логарифму в групі точок гіпереліптичної кривої.

1. За типом криптографічної системи:

* Симетричні цифрові підписи – цифрові підписи, що ґрунтуються на симетричних криптографічних перетвореннях з використанням третьої довірчої сторонни;
* Асиметричні цифрові підписи – цифрові підписи, що ґрунтуються на асиметричних криптографічних перетвореннях і можуть здійснюватись:
* з використанням третьої довірчої сторони;
* без використання третьої довірчої сторони.

1. За мірою використання криптографічного перетворення типу «шифрування»:

* цифрові підписи з використанням шифрування;
* цифрові підписи без використання шифрування.

1. За характером виконуваного цифрового підпису:

* детерміновані цифрові підписи;
* одноразового чи багаторазового застосування;
* цифрові підписи з рандомізацією.

У RSA системі як загальносистемний параметр використовується модуль .

У користувачів модулі  мають бути різними.

Електронний цифровий підпис обчислюється на основі відкритого,

де  – ключ ЕЦП. Ключі *Еk* та *Dk* є пов’язаними між собою

Перевірка ЕЦП. При перевірці користувач, що володіє відкритим ключем , знаходить ВЕП: .

Після цього перевіряючий має всю інформацію про хеш – функцію та параметри:.

На основі аналізу складових  контролюється цілісність та достовірність.

Стійкість ЕЦП залежить від складності факторизації модуля *Nj* на прості числа *Pj* та *Qj*.

**8. Які методи існують та які з них краще застосовувати для дискретного логарифмування в групі точок еліптичної кривої?**

Найбільш слабким ланцюгом цифрових підписів в полі Галуа є субекспоненціальна складність розв’язання дискретного логарифма, тобто знаходження особистого ключа *х*а при відомих відкритому ключі *Yа* та модулі перетворення *Р*. Суттєво підвищення стійкості може бути здійснене за рахунок використання перетворень в групі точок еліптичних кривих. У цьому випадку стійкість визначається складністю розв’язку порівнянь  для розширеного поля, або  для еліптичної кривої над простим полем. Для вирішення дискретного логарифмічного рівняння жожна скористатить методом Поларда. Нехай необхідно вирішити дискретне логарифмічне рівняння: . Скористаємося методом Поларда, і вважатимемо, що ми знайшли деяку пару параметрів (*u,v*) і (*t,w*), таких що: .  Підставимо в порівняння значення *b*: , . У рівнянні (1.170) можна прирівняти показники, але за модулем функції Ейлера від , тобто:



За допомогою - методу Поларда сформуємо значення , тобто задамо правило, аналогічне з правилом розподілу на область:

, де . Для розв’язання дискретного логарифма метод - Поларда є обчислювально складним (при „сильних” *P* субекспоненційно)., але іноді і максимально зручним.

Існує також схема Діффі-Хеллмана розв\*язку дискретного логарифмічного рівняння:

*x*=log*QY*(mod*P*).

// Для ЕК складність розв’язання задачі дискретного еліптичного рівняння, визначається числом операцій додавання в групі точок ЕК:

, де  – порядок базової точки ЕК.

**9-. Сутність алгоритму ЕЦП, що ґрунтується на перетвореннях в скінченному полі та які його властивості?**

Алгоритми ЦП FIPS 186-1 (DSA) та ГОСТ Р 34. 10-94 [60, 57] дуже схожі та пройшли випробовування часом. Ці алгоритми і зараз застосовуються дуже широко. Так, у FIPS 186-3 [63] передбачається продовжити використання DSA. По суті, в них використовується криптографічний алгоритм перетворення Ель-Гамаля за двома модулями – простими числами P та q. Загальносистем­ними параметрами з урахуванням позначень у стандартах є для DSA, або  – для ГОСТ Р 34.10-94, де Р – просте «сильне» число, q – також просте число, але яке входить до канонічного розкладу числа (Р – 1), а g(а) – первісний елемент простого поля. У табл. 6.7 наведено вимоги щодо цих загальносистемних параметрів.

*Таблиця 6.7*

**Загальні параметри ЦП у простому полі Галуа**

|  |  |
| --- | --- |
| **DSA** | **ГОСТ Р 34. 10-94** |
|  |  |
| **Р – просте число,**  **і може змінюватися з кроком** |  |
| **q – просте число,** |  |
|  | |
| **1 < g < p** | **1 < a < p** |
|  |  |

Указані загальносистемні параметри можуть бути для всіх користувачів однаковими і змінюватися дуже рідко. У FIPS 186-1 обмеження на загальні параметри інші. Алгоритми вироблення й перевірки підпису розглянемо на прикладі DSA-подібного ЦП згідно з ГОСТ 34.310-96.

Електронний цифровий підпис в полі Галуа

Сутність методу Ель-Гамаля

Протокол розповсюдження ключів

Нехай є суб’єкти *А* та *В*, які мають таємні ключі випадкової послідовності *ХА* та *ХВ*, а також відкриті ключі *YА* та *YВ*:

, (15.8)

. (15.9)

Відкриті ключі розповсюджуються в системі з забезпеченням їх цілісності та справжності.

Перевіряння підпису:

, (15.10)

де  – загальний параметр;

 – відкритий ключ підписувача;

k – особистий сеансів ключ (таємний та формується відправником).

, (15.11)

де , r- відкритий сеансів ключ.

Розв’яжемо (15.10) та знайдемо :

; (15.12)

; (15.13)

; (15.14)

. (15.15)

Захищене повідомлення в системі Ель - Гамаля, підписане автором:

. (15.16)

Перевіряння цілісності та справжності

Об’єкт, що перевіряє має :

- обчислюється ;

- усі параметри підставляються в (15.10). Якщо порівняння справедливо, тобто:

,

то повідомлення цілісне та справжнє.

Проблемні питання реалізації різних криптоперетворень:

1. всі операції виконуються з великими цілими числами;
2. генерування загальних параметрів для кілець, полів Галуа, груп точок еліптичних кривих, груп точок гіпереліптичних кривих, відображення точок еліптичних кривих;
3. скалярного множення в групах точок еліптичних та гіпереліптичних;

4) обчислення парних відображень типу спарювання точок еліптичних кривих тощо.

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

Вважається, що абсолютну частку обчислювальної складності криптоаналізу RSA становить розв’язання задачі факторизації модуля перетворення. Тому задачу криптоаналізу RSA зводять до задачі розкладання (факторизації) модуля N на два простих числа – P та Q.

**30.3.1. Методика криптоаналізу RSA**

Вважається [236, 422, 11, 13], що найбільш ефективною (можливо) є така методика визначення RSA особистого ключа, наприклад *Ek* для цифрового підпису або *Dk* для направленого розшифрування k – го користувача.

Розглянемо загальну методику криптоаналізу стосовно визначення особистого ключа.

Вхідні дані – відкритий параметр – модуль перетворення *Nj* = P Q та відкритий ключ (сертифікат) ЦП *Di*. Конфіденційними параметрами є прості числа P та Q і відповідно значення функції Ойлера:

*= *, (9.1)

а також особистий ключ ЦП *Ei*.

З урахуванням наведеного, криптоаналіз RSA може бути виконаний згідно з такою методикою.

1. Криптоаналітик відповідним чином отримує дані про RSA криптосистему.

2. Криптоаналітик отримує відповідним чином відкриті параметри та відкритий ключ (сертифікат), тобто вхідні дані, що наведені вище.

3. Здійснюється факторизація модуля перетворення відповідного користувача Ni на два прості числа P та Q. Це найскладніший етап.

4. При відомих простих числа P та Q обчислюється значення функції Ойлера

*= .*

5. При відомих значеннях  та відкритому ключі *Di* розв’язується порівняння *k*-користувача відносно особистого ключа *Ek*:

. (9.2)

Наведемо також історію розв’язання задачі факторизації. Для великих  з великими простими множниками розкладання на множники є серйозною проблемою. Разючою ілюстрацією цього може служити така історія [236]. У 1977 році три винахідники алгоритму RSA наважилися запропонувати читачам популярного журналу Scientific American дешифрувати направлено зашифроване повідомлення. Мартін Гарднер опублікував у журналі Scientific American зашифровану головоломку, для розшифрування якої потрібно було факторизувати RSA модуль перетворення – таке 129-розрядне число (428 бітів) [236, 11]:

N129= 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.

Повідомлення «The magic words are squeamish ossifrage», яке потрібно було зашифрувати, спочатку було записане у вигляді цілого числа (а = 01, b = 02, c = 03, …, z = 26, прогалина, 00). Потім воно було зашифроване направлено на відкритому ключі *Ek* = 9007. Наведені модуль перетворення та відкритий ключ, а також додаткова інформація що, N = P×Q, де P і Q – прості числа, довжиною відповідно 64- та 65-десяткових розрядів, були опубліковані в указаному журналі.

За розшифровку цього повідомлення вони запропонували нагороду в 100 дол. За їхніми оцінками, задача не могла бути розв’язана раніше, ніж приблизно через 40 квадрильйонів років [236]. Але у квітні 1994 року D. Atkins, M. Graff, K. Lenstra і C. Leylang зажадали виплати призової суми за успішний криптоаналіз усього після восьми місяців спільної роботи в Internet. Для розв’язання задачі факторизації зазначеного модуля було використано 1600 комп’ютерів різної потужності – від найпростіших до станції Gray C90. Задача факторизації, яка вимагала близько 5000 міпсороків, була розв’язана із серпня 1993 по квітень 1994 року із застосуванням квадратичного решета. Одиницею вимірювання складності задачі в даному випадку є MIPS-рік – обсяг роботи, що виконується протягом року процесором, що здійснює обробку одного мільйона команд у секунду, що приблизно еквівалентно виконанню 3×1013 команд. Так, машина на базі Pentium з частотою 2000 МГц показує швидкість 500 MIPS.

Таким чином, були визначені прості конфіденційні числа P та Q, причому [236, 11]:

P = 3490529510847650949147849619903898133417764638493387843990820577,

Q = 327691329932667095499619881908344614131177642967992942539798288533.

З квітня 1996 по квітень 2003 року були розв’язані задачі для RSA-130, RSA-140, RSA-155, RSA-160. Не факторизованим залишився лише RSA-150, але він у подальшому був відкликаний з переліку задач.

Останньою з розв’язаних задач є задача для RSA-232, у якій довжина ключа дорівнює 768 бітів. Групі вчених із Германії, Нідерландів, США, Франції, Швейцарії та Японії у 2009 році вдалося дешифрувати повідомлення, що було зашифроване на ключі 768 бітів згідно із стандартом RSA. Для цього було застосоване загальне решето числового поля. Згідно даних [423], на перший крок для вибору поліномів 1 та 6 степенів було витрачено близько півроку і працювали 80 процесорів. На головний етап просіювання було потрачено близько двох років і використано сотні комп’ютерів різної потужності. Якби цю задачу розв’язували на одному процесорі AMD Optron 2.2 ГГц, то потрібно було б 1500 років його роботи. На третьому етапі обробка даних із розв’язанням задачі лінійної алгебри тривала декілька тижнів. Знаходження нетривіальних рішень здійснювалося на декількох незалежних кластерах протягом понад три місяці. Обсяг прорідженої матриці складав 192 796 550×192 795 550 елементів, причому ненульових було 27 795 115 920 елементів. Для зберігання матриці на жорсткому диску знадобилося близько 105 гігабайтів та близько 5 терабайтів для зберігання стиснутих даних при побудуванні такої матриці.

*Таблиця 9.3*

Прогрес у розв’язку задач факторизації модуля *N*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Число десяткових знаків | Приблизне число бітів | Дата розв’язання | Необхідне число MIPS-років | Використаний алгоритм |
| 100 | 332 | 1991 р. | 7 | Квадратичне решето |
| 110 | 365 | 1992 р. | 75 | Квадратичне решето |
| 120 | 398 | 1993 р. | 830 | Квадратичне решето |
| 129 | 428 | 1994 р. | 5000 | Квадратичне решето |
| 130 | 431 | 1996 р. | 500 | Загальне решето числового поля |
| 140 | 464 | 1999 р. |  | Загальне решето числового поля |
| 153 | 512 | 1999 p. | 8000 | Загальне решето числового поля |
| 155 | 514 | 1999 р. |  | Загальне решето числового поля |
| 160 | 531 | 2003 р. |  | Загальне решето числового поля |
| 174 | 576 | 2003 р. |  | Загальне решето числового поля |
| 199 | 663 | 2005 | 1.28×105 | Загальне решето числового поля |
| 232 | 768 | 2009 | 4×106 | Загальне решето числового поля |
| 270 | 896 | Відкритий |  |  |
| 309 | 1024 | Відкритий |  |  |
| 463 | 1536 | Відкритий |  |  |
| 617 | 2048 | Відкритий |  |  |

Для розкладання на множники до 1994 року застосовувався підхід, відомий як метод квадратичного решета. Для криптоаналізу RSA-130, RSA-140, RSA-155, RSA-160, RSA-174 використовувався новий алгоритм, названий методом решета в полі чисел загального вигляду, що дозволило скоротити обсяг обчислювальних зусиль майже на 10% у порівнянні з тими, що були потрібні раніше для аналізу RSA-129. Як випливає із табл. 9.3, новими успіхами факторизації стали модулі RSA-199 (663 бітів) та RSA-232 (768 бітів) [423]. Задачі факторизації RSA від RSA-270 (896 бітів) до RSA-617 (2048 бітів) залишаються відкритими, з нагородами відповідно від $ 20000 до $ 200000 [423].

Необхідно відзначити, що загроза ключам великої довжини подвійна, з одного боку – безупинне зростання обчислювальної потужності сучасних комп’ютерів, а з іншого – безупинне вдосконалення математичних методів розкладання на множники. Важливими також є певні сподівання на розв’язання задач факторизації на основі квантових обчислень, стан і деякі питання їх реалізації розглядаються нижче.

**Основні методи факторизації RSA**

З появою алгоритму RSA послідовно з часом були розроблені та реалізовані ряд методів факторизації модуля перетворення *N* [236, 422, 423, 11, 421, 4, 96, 9–13]. У цілому методи факторизації можна поділити на два великих класи – з експоненційною та субекспоненційною складністю. Окремо можна розглядати поліноміальний метод (Гордона Чалмерса) [421].

До експоненційно складних належать такі методи:

* перебирання типу «груба сила» зі складністю О(N1/2);
* ρ-Полларда метод зі складністю О(N1/4);
* P–1 Полларда метод;
* P+1 метод Вільямса;
* метод квадратичних форм Шенкса зі складністю О(N1/4);
* метод Лемана.

До субекспоненційни[методів належать:

* метод Діксона зі складністю LN(1/2, 2);
* метод безперервних дробів зі складністю LN(1/2, );
* метод квадратичного решета зі складністю LN(1/2, );



* метод еліптичних кривих зі складністю Lp(1/2, ), де P – найменше просте, яке ділить N;
* метод решета числового поля зі складністю LN(1/3,(64/9)1/3);
* метод спеціального решета числового поля зі складністю LN(1/3,(32/9)1/3).

Окремо необхідно назвати с.