13. Методи та засоби забезпечення передачі інформації в АСУ. Загрози, яким підлягає інформація. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту.

13.1. Загрози, яким підлягає інформація.

Як показує аналіз , сучасні комп'ютерні системи підлягають наступним найбільш розповсюдженим загрозам:

- ненавмисні помилки користувачів, операторів, системних адміністраторів і інших осіб (65%)
- крадіжки і фальсіфікація В більшості випадків, що розслідувалися, винними виявлялися штатні співробітники організацій, відмінно знайомі із режимом роботи і мірами захисту;
- "ображені співробітники" - нинішні і колишні, наприклад, шляхом вживлення "логічної бомби", введення невірних даних, вилучення або модифікації даних;
- загрози від навколишньої середи(відключення зв'язку, пожежа і т.і.);
- дії хакерів і злочинців, що можуть здійснювати обман шляхом створення неправдивих або модифікованих справжніх документів (інформації).

В процесі реалізації загроз порушники і злочинці можуть реалізовувати наступні **стратегії**:

а) видавання себе за іншого користувача, щоб зняти з себе відповідальність;

б) видавання себе за іншого користувача, щоб використовувати його повноваження з метою:

1) формування неправдивої інформації;
2) зміни істинної інформації;
3) застосування неправдивого посвідчення для отримання несанкціонованого доступу (НСД);
4) санкціонування неправдивих обмінів інформацією або іхнє підтвердження;

в) відмова джерела від факту формування і передачі інформації;

г) твердження джерела про те, що одержувачу була відправлена інформація, в тому числі в певний час, що насправді не була відправлена або відправлена в інший час;

д) відмова отримувача від факту отримання інформації, хоча насправді вона була отримана, або неправдиве затвердження про час її отримання;

е) твердження про те, що інформація отримана від певного користувача, хоча насправді вона сформована самим же порушником;

є) отримання НСД, тобто порушення конфіденційності інформації, що захищається;

ж) несанкціоноване розширення (зміна) своїх повноважень;

з) несанкціонована зміна повноважень інших осіб (обмеження або розширення);

и) введення в систему або активізація вірусів або інших "шкідливих" програм з метою перехоплення ключів і паролів, а також модифікації (непомітно) документів;

і) спроба завадити передачі повідомлень між іншими користувачами, в частковості, внесення до повідомлення прихованих завад для того, щоб це повідомлення при автентифікації було спростоване;

ї) модифікація програмного забезпечення, наприклад, шляхом додання нових функцій;

й) підрив довіри до протоколу шляхом виклику порушень або примушення інших порушити протокол шляхом введення неправдивої інформації і т.і.

13.2. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту.

Перекриття більшості названих загроз може бути здійснено за рахунок формування і проведення в життя **політики безпеки** - набору законів , правил і норм поведінки, які визначають те, як АСУ обробляє, захищає і розповсюджує інформацію. По суті **політика безпеки** - це активний компонент захисту, що включає в себе аналіз можливих загроз і вибір мір протидії. В практичному додатку політика безпеки являє собою сукупність документованих управлінських рішень, направлених на захист інформації і асоційованих з нею ресурсів. В результаті реалізації такої політики повинна бути створена система захисту інформації, що являє собою комплекс організаційних, технічних засобів і заходів, юридичних, законодавчих норм, фізичних обмежень і т.і., які реалізуються комплексно на всіх етапах життєвого циклу інформаційної системи : від проектування - і до застосування в різноманітних умовах.

В СЗІ повинні реалізовуватися функції безпеки і механізми безпеки; вони повинні перекривати всі виявлені загрози, перераховані вище.

Перелік основних задач, які повинні вирішуватися системою комп'ютерної безпеки:

•керування доступом користувачів до ресурсів АСУ, з метою її захисту від неправомірного випадкового або навмисного втручання у роботу системи і несанкціонованого (із перевищенням наданих повноваженнь) доступу до її інформаційних, програмних і апаратних ресурсів із боку стороніх особ, а також осіб із числа персоналу організації і користувачів;

•захист даних, що передаються по каналам зв'язку;

•реєстрація, збір, збереження, опрацювання і видача даних про усі події, що відбувалися у системі і мали відношення до її безпеки;

• контроль роботи користувачів системи з боку адміністрації і оперативне оповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

•контроль і підтримка цілісністності критичних ресурсів системи захисту і середовища виконання прикладних програм;

•забезпечення замкнутого середовища перевіреного програмного забезпечення, із метою захисту від безконтрольного впровадження у систему потенційно небезпечних програм (у яких можуть міститись вредоносні закладки або небезпечні

помилки) і засобів подолання системи захисту, а також від впровадження і поширення комп'ютерних вірусів;

•керування засобами системи захисту.

Звичайно розрізняють зовнішню і внутрішню безпеку комп'ютерних систем. **Зовнішня безпека** включає захист АСУ від стихійного лиха (пожежи, повіні і т.п.) і від проникнення у систему зловмисника ззовні з цілями розкрадання, одержання доступу до інформації або виводу системи з ладу. **Внутрішня безпека** – створення надійних і зручних механізмів регламентації діяльністі усіх її законних користувачів і обслуговуючого персоналу для примусу їх до безумовного дотримання встановлених в організації дисципліни доступу до ресурсів системи.

Міри протидії погрозам безпеки. Класифікація мір забезпечення безпеки комп'ютерних систем

По спосібу здійснення усі міри забезпечення безпеки комп'ютерних систем підрозділяються на: правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні і технічні (апаратурні і програмні).

До **правових** мір захисту відносяться діючі у країні закони, укази і нормативні акти, що регламентують правила роботи з інформацією

До **морально-етичних** мір протидії відносяться норми поводження, що традиційно склались або складаються у міру поширення ЕОМ у країні або суспільстві.

Організаційні (адміністративні) міри захисту - це міри організаційного характеру, що регламентують процес функціонування системи опрацювання даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів з системою таким чином, щоб найбільшою мірою утруднити або виключити можливість реалізації погроз безпеки.

Фізичні міри захисту засновані на застосуванні різного роду механічних, электро- або електронно-механічних пристроїв і спорудженнь, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонент системи і захищаємої інформації, а також технічні засоби візуального спостереження, зв'язку і охоронної сигналізації

Технічні (апаратно-програмні) міри захисту засновані на використанні різних електронних пристроїв і спеціальних програм, що входять до складу АСУ і виконують (самостійно або в комплексі з іншими засобами) функці захисту (ідентифікацію й автентификацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічне закриття інформації і т.д.)

Основні принципи побудови систем захисту АСУ

Захист інформації в АСУ повинний грунтуватися на наступних основних принципах:

•системності,

•комплексності;

•безперервності захисту;

•розумної достатності;

•гнучкості керування і застосування:

•відкритості алгоритмів і механізмів захисту;

•простоти застосування захисних мір і засобів.

Принцип системності

Системний підхід припускає необхідність обліку усіх взаємозалежних, взаємодіючих і елементів, які змінюються в часу, умов і чинників, значимих для розуміння і рішення проблеми забезпечення безпеки АСУ.

Принцип комплексності

У розпорядженні фахівців із комп'ютерної безпеки є широкий спектр мір, методів і засобів захисту комп'ютерних систем. Комплексне їхнє використання припускає погоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекриває всі істотні канали реалізації погроз і не має слабких місць на стиках окремих її компонентів**.**

Принцип безперервності захисту

Захист інформації - це безупинний цілеспрямований процес, що припускає прийняття відповідних мір на всіх етапах життєвого циклу АСУ, починаючи із самих ранніх стадій проектування, а не тільки на етапі її експлуатації**.**

Розумна достатність

Створити абсолютно непереборну систему захисту принципово неможливо. При достатній кількості часу і засобів можна перебороти будь-який захист. Тому має сенс вести мову тільки про деякий прийнятний рівень безпеки.

Гнучкість системи захисту

Для забезпечення можливості варіювання рівнем захищеності, засоби захисту повинні мати визначену гнучкість. Особливо важливим ця властивість є в тих випадках, коли установку засобів захисту необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування.

Відкритість алгоритмів і механізмів захисту

Суть принципу відкритості алгоритмів і механізмів захисту перебуває в тому, що захист не повинний забезпечуватися тільки за рахунок таємності структурної організації й алгоритмів функціонування її підсистем

Принцип простоти застосування засобів захисту

Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути зв'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових трудозатрат при звичайній роботі законних користувачів, а також не повинно жадати від користувача виконання рутинних малозрозумілих йому операцій (введення кількох паролів і імен і т.д.).

Основні механізми захисту комп'ютерних систем від проникнення з метою дезорганізації їхньої роботи і НСД до інформації

Затвердимо ряд понять, необхідних надалі .

1. Об'єкт - пасивний компонент системи, одиниця ресурсу автоматизованої системи (пристрій, диск, каталог, файл і т.п.), доступ до якого регламентується правилами розмежування доступу.

2. Суб'єкт - активний компонент системи (користувач, процес, програма), дії якого регламентуються правилами розмежування доступу.

3. Доступ до інформації - ознайомлення з інформацією, (копіювання, тиражування), її модифікація (коректировка) або знищення (видалення).

4. Доступ до ресурсу - одержання суб'єктом можливості маніпулювати (використовувати, управляти, змінювати характеристики і т.п.) даним ресурсом.

5. Правила розмежування доступу - сукупність правил, що регламентують права доступу суб'єктів до об'єктів у деякій системі.

6. Розмежування доступу до ресурсів АСУ - це такий порядок використання ресурсів автоматизованої системи, при якому суб'єкти одержують доступ до об'єктів у суворій відповідності з установленими правилами.

7. Авторизований суб'єкт доступу - суб'єкт, якому надані відповідні права доступу до об'єктів системи (повноваження).

8. Несанкціонований доступ (НСД) - доступ суб'єкта до об'єкта в порушення встановлених у системі правил розмежування доступу.

9. Несанкціонована дія - дія суб'єкта в порушення встановлених у системі правил обробки інформації.

Для реалізації наведених вище мір захисту комп'ютерних систем використовуються **універсальні механізми захисту інформації**. До числа таких механізмів відносяться:

• ідентифікація (найменування і впізнання), автентифікація (підтвердження істинності) і авторизація (присвоєння повноважень) суб'єктів;

• контроль (розмежування) доступу до ресурсів системи;

• реєстрація й аналіз подій, що відбуваються в системі;

• контроль цілісності ресурсів системи.

Механізми ідентифікації, автентифікації й авторизації необхідні для підтвердження істинності суб'єкта, забезпечення його роботи в системі, і визначення законності прав суб'єкта на даний об'єкт або на визначені дії з ним.

Ідентифікація - це процес розпізнавання елемента системи, зазвичай за допомогою заздалегідь визначеного ідентифікатора або іншої унікальної інформації; кожний суб'єкт або об'єкт системи повинний бути однозначно ідентифіцуємим.

Автентифікація - це перевірка істинності ідентифікації користувача, процесу, пристрою або іншого компоненту системи (звичайно здійснюється перед дозволом доступу); а також перевірка цілісності й авторства даних при їхньому збереженні або передачі для запобігання несанкціонованої модифікації.

Авторизація - це надання суб'єкту прав на доступ до об'єкта.

13.3. Криптографічні методи захисту. Види засобів криптозахисту даних. Переваги і недоліки. Місце і роль засобів криптозахисту.

Криптографічні методи захисту засновані на можливості здійснення деякої операції перетворення інформації, що може виконуватися одним або декількома користувачами АСУ, які володіють деякою таємною частиною додаткової

інформації, без знання якої з великою імовірністю, неможливо здійснити цю операцію .

У **класичній криптографії (симметричній)** використовується тільки одна одиниця конфіденційної й обов'язково таємної інформації - ключ, знання якого дозволяє відправнику зашифрувати інформацію, а одержувачу - розшифрувати її. Саме ця операція зашифрування/расшифрування з великою імовірністю нездійсненна без знання таємного ключа.

У **криптографії з відкритим ключем (несимметричній, асиметричній)** є два ключі, принаймні один із яких не можна обчислити з іншого. Один ключ використовується відправником для зашифрування інформації, цілість якої повинна бути забезпечена. Інший ключ використовується одержувачем для опрацювання отриманої інформації. Бувають додатки, у яких один ключ повинний бути нетаємним, а іншій - таємним.

Криптографічні методи захисту дозволяють вирішувати наступні задачі:

•закриття даних, збережених в АСУ або переданих по каналах зв'язку;

•контроль цілісності й автентичності даних, переданих по каналах зв'язку. Основною **перевагою** криптографічних методів захисту інформації є те, що вони забезпечують гарантовану стійкість захисту, що можна розрахувати і висловити в числовій формі (середнім числом операцій або кількістю часу, необхідного для розкриття зашифрованної інформації або обчислення ключів).

Однак, криптографічні методи володіють і істотними **недоліками**, до числа яких можна віднести наступні:

•низька швидкодія існуючих алгоритмів шифрування (ДСТ 28147-89, ДСТУ 4145-2002, та інші.);

•труднощі зі спільним використанням зашифрованної інформації;

•високі вимоги до цілості таємного ключа;

•труднощі з застосуванням у відсутності засобів захисту від НСД.

Ці недоліки принципово переборні. Однак їхнє подолання може привести до повної непрацездатності системи захисту.

Засоби шифрування можуть бути реалізовані як апаратно, так і чисто програмно. У будь-якому випадку вони повинні бути сертифіцированими, тобто повинні відповідати визначеним вимогам (стандартам) . У противному випадку, вони не можуть гарантувати користувачам необхідну стійкість шифрування.

Використання в системі захисту для різних цілей декількох однотипних алгоритмів шифрування нераціонально. Оптимальним варіантом можна вважати таку систему, у якій засоби криптозахисту загальносистемні, тобто виступають у якості розширення функцій операційної системи і включають сертифіцировані алгоритми шифрування всіх типів (блокові і потокові, із закритими і відкритими ключами) .

Доцільно застосування **криптографічних** методів захисту для рішення наступних задач :

•для автентифікації користувачів системи (особливо віддалених);

•для закриття і контролю цілісності інформації, переданої по каналах зв'язку;

•для закриття конфіденційної інформації в АСУ (на системному рівні для захисту критичної інформації операційної системи і самої системи безпеки, на прикладному рівні - для закриття таємної і конфіденційної інформації користувачів).

За допомогою криптографічних методів можливо:

- шифрування інформації;
- реалізація електронного підпису;
- розподіл ключів шифрування;
- захист від випадкової або навмисної зміни інформації.

До алгоритмів шифрування пред'являються наступні вимоги:

- високий рівень захисту даних проти дешифрування і можливої модифікації;
- захищеність інформації повинна засновуватися тільки на знанні ключа і не залежати від того, відомий алгоритм або ні;
- мала зміна вихідного тексту або ключа повинна приводити до значної зміни шифрованого тексту (ефект "обвалу");
- область значень ключа повинна виключати можливість дешифрування даних шляхом перебору значень ключа;
- економічність реалізації алгоритму при достатній швидкодії;
- вартість дешифрування даних без знання ключа повинна перевищувати вартість даних.

Перед шифруванням інформацію варто піддати статистичному кодуванню (стиску, архівації). При цьому зменшиться об'єм інформації і її надмірність, підвищиться ентропія (середня кількість інформації, що доводитися на один символ). Тому що в стиснутому тексті будуть відсутні повторювані літери і слова, дешифрування (криптоаналіз) вагається.

Класифікація алгоритмів шифрування

1. Симетричні (із секретним, єдиним ключем, одноключові, single-key).

1.1. Потокові (шифрування потоків даних):

- з одноразовим або безкінечним ключем (infinite-key cipher);
- с кінцевим ключем (система Вернама - Vernam);
- на основі генератора псевдослучайних чисел (ПСЧ).

1.2. Блокові (шифрування даних поблочно):

1.2.1. Шифри перестановки (permutation, P-блоки);

1.2.2. Шифри заміни (підстановки, substitution, S-блоки):

- моноалфавитні (код Цезаря);
- поліалфавитні (шифр Видженера, циліндр Джефферсона, диск Уэтстоуна, Enigma);

1.2.3. складові :

- DES (Data Encryption Standard, США);
- Lucipher (фірма IBM, США);
- FEAL-1 (Fast Enciphering Algoritm, Японія);

- IDEA/IPES (International Data Encryption Algorithm/
- Improved Proposed Encryption Standard, фірма Ascom-Tech AG, Швейцарія);
- B-Crypt (фірма British Telecom, Великобританія);
- ДСТ 28147-89 (СРСР);
- Skipjack (США).

2. Асиметричні (із відкритим ключем, public-key):

- Диффи-Хеллман DH (Diffie, Hellman);
- RSA (Rivest, Shamir, Adleman); (стандарт ISO-MKKTT X-509), RSA-PSS;
- Эль-Гамаль ElGamal (DSA (X9.30)) ;
- ACE-Sign;
- Flash, Sflash;
- Quartz;
- ESIGN;
- Цифровий підпис DSS (P1363), Шнора, EC-DSA – GF(p), EC-DSA – GF(2^m), ECSS, EC-GDSA Германії, EC-KCDSA Кореї, ДСТ Р.34.310-95 Росії, ДСТ Р.3410-2001 Росії , ДСТУ 4145-2002 України. Починаючи з алгоритму Шнора, використовуються перетворення в групі точок еліптичних кривих.

Крім того, є поділ алгоритмів шифрування на власне шифри (ciphers) і коди (codes). Шифри працюють з окремими бітами, літерами, символами. Коди оперують лінгвістичними елементами (склади, слова, фрази).

Симетричні алгоритми шифрування

Симетричні алгоритми шифрування (або криптографія із секретними ключами) засновані на тому, що відправник і одержувач інформації використовують той же самий ключ. Цей ключ повинен зберігатися в таємниці і передаватися способом, що виключає його перехоплення. Обмін інформацією здійснюється в 3 етапи:

- відправник передає одержувачу ключ (у випадку мережі з декількома абонентами в кожній парі абонентів повинен бути свій ключ, відмінний від ключів інших пар);
- відправник, використовуючи ключ, зашифровує повідомлення, що пересилається одержувачу;
- одержувач одержує повідомлення і розшифровує його.

Якщо для кожного дня і для кожного сеансу зв'язку буде використовуватися унікальний ключ, це підвищить захищеність системи.

Потокові шифри

У потокових шифрах, тобто при шифруванні потоків даних, кожний біт вихідній інформації шифрується незалежно від інших за допомогою гаммування. **Гаммування** - накладення на відкриті дані гамми шифру (випадкової або псевдовипадкової послідовності одиниць і нулів) по визначеному правилу. Звичайно використовується " щовиключає АБО", називане також додаванням по

модулю 2 і реалізоване в ассемблерних програмах командою XOR. Для расшифровування та ж гама накладається на зашифрованні дані. При однократному використанні випадкової гами однакового розміру з тими що зашифровуються даними, злом коду неможливий (так називані криптосистеми з одноразовим або безкінечним ключем). У даному випадку "безкінечний" означає, що гама не повторюється. У деяких потокових шифрах ключ коротше повідомлення. Часто використовують гаму, одержувану за допомогою генератора псевдослучайних чисел (ПСЧ). У цьому випадку ключ - число, що породжує, (початкове значення, вектор ініціалізації, initializing value,) для запуску генератора ПСЧ. Кожний генератор ПСЧ має період, після якого послідовність що генерується повторюється. Вочевидь, що період псевдослучайної гами буде більше довжини інформації що шифрується

Блокові шифри

При блоковому шифруванні інформація розбивається на блоки фіксованої довжини і шифрується поблочно. Блокові шифри бувають двох основних видів:

- шифри перестановки (transposition, permutation, P-блоки);
- шифри заміни (підстановки, substitution, S-блоки).

Шифри перестановок переставляють елементи відкритих даних (біти, літери, символи) у деякому новому порядку. Розрізняють шифри горизонтальної, вертикальної, подвійної перестановки, штахети, лабіринти, лозунгові й ін. Шифри заміни заміняють елементи відкритих даних на інші елементи по визначеному правилу. Розрізняють шифри простої, складної, парной заміни, буквено-складове шифрування і шифри колоною заміни. Шифри заміни діляться на дві групи:

- моноалфавитні (код Цезаря) ;
- поліалфавитні (шифр Видженера, циліндр Джефферсона, диск Уэтстоуна, Enigma).

У моноалфавитних шифрах заміни літера вихідного тексту заміняється на іншу, заздалегідь визначену літеру.

У поліалфавитних підстановках для заміни деякого символу вихідного повідомлення в кожному випадку його появи послідовно використовуються різні символи з деякого набору.

У сучасних криптографічних системах, як правило, використовують обидва способи шифрування (заміни і перестановки). Такий шифратор називають складовим (product cipher). Він більш стійкий, чим шифратор, що використовує тільки заміни або перестановки. **Блокове шифрування** можна здійснювати **подвійно:**

1. Без зворотного зв'язку (ЗЗ). Прикладами є DES у режимі ECB і ДСТ 28147-89 у режимі простої заміни.

2. З зворотним зв'язком. Приклад - DES у режимі CBC.

DES передбачає 4 режими роботи:

- ECB (Electronic Codebook) електронний шифрблокнот;
- CBC (Cipher Block Chaining) ланцюжок блоків;
- CFB (Cipher Feedback) зворотний зв'язок по шифртексту;

- OFB (Output Feedback) зворотний зв'язок по виходу.

ДСТ 28147-89 - вітчизняний стандарт на шифрування даних. Стандарт включає три алгоритми зашифрування (розшифрування) даних:

- режим простої заміни, режим гаммування,
- режим гаммування зі зворотним зв'язком
- режим випрацювання імітовставки. За допомогою імітовставки можна зафіксувати випадкову або навмисну модифікацію зашифрованної інформації.

Алгоритми шифрування ДСТ 28147-89 мають гідності інших алгоритмів для симетричних систем і перевершують їх своїми можливостями. Так, ДСТ 28147-89 (256-бітовий ключ, 32 циклу шифрування) у порівнянні з такими алгоритмами, як DES (56-бітовий ключ, 16 циклів шифрування) і FEAL-1 (64-бітовий ключ, 4 цикли шифрування) має більш високу криптостійкість за рахунок більш довгого ключа і більшого числа циклів шифрування. Слід зазначити, що на відміну від DES , у ДСТ 28147-89 блок підстановки можна довільно змінювати, тобто він є додатковим 512-бітовим ключем. Алгоритми гаммування ДСТ 28147-89 (256-бітовий ключ, 512-бітовий блок підстановок, 64-бітовий вектор ініціалізації) перевершують по криптостійкості й алгоритм B-Crypt (56-бітовий ключ, 64-бітовий вектор ініціалізації). Гідностями ДСТ 28147-89 є також наявність захисту від нав'язування помилкових даних (випрацюання імітовставки) і однаковий цикл шифрування у всіх чотирьох алгоритмах ДСТ. Блокові алгоритми можуть використовуватися і для виробітки гами. У цьому випадку гама випрацьовується блоками і поблочно складається по модулю 2 із вихідним текстом. Як приклад можна назвати B-Crypt, DES у режимах CFB і OFB, ДСТ 28147-89 у режимах гаммування і гаммуання з зворотним зв'язком.

Асимметричні алгоритми шифрування

У асиметричних алгоритмах шифрування (або криптографії з відкритим ключем) для зашифровування інформації використовують один ключ (відкритий), а для расшифрування - інший (секретний). Ці ключі різні і не можуть бути отримані один з іншого. Схема обміну інформацією така:

- одержувач обчислює відкритий і секретний ключі, секретний ключ береже в таємниці, відкритий же робить доступним (повідомляє відправнику, групі користувачів мережі, публікує);
- відправник, використовуючи відкритий ключ одержувача, зашифровує повідомлення, яке пересилається одержувачу;
- одержувач одержує повідомлення і розшифровує його, використовуючи свій секретний ключ.

На теперішній час найпоширеніші три підкласи несиметричних систем, стійкість яких базується відповідно на складності факторизації числа великої розрядності, знаходження дискретного логарифма у кінцевих полях і знаходження дискретного логарифма в групі точок еліптичних кривих.

До першого класу відноситься RSA-подібні шифри, до другого Диффі-Хеллманн та Ель-гамаль, до третього, алгоритмиперераховані у останньому пункту класифікації алгоритмів приведеної вище.