*Екзаменаційна робота*

*З дисципліни Прикладна криптологія*

*Студента 3 курсу ФКН гркупи КБ-31*

*Кравчека Євгена*

*Білет №12*

1. Сутність атаки повне розкриття та її ефективність відносно асиметричних криптосистем в групі точок ЕК.

Повне розкриття – противник отримує сектертній ключ користувача. Сутність атаки повне розкриття міститься в розв’язку дискретних логарифмічних рівнянь. Якщо криптоаналітик визначить секретний ключ, то вподальшому вн зможе нав’язувати хибні загальні секрети та хибні повідомлення. Для суттєвого ускладнення можливості нав язування хибних загальних секретів використовують як довгострокові, так і сеансові загальні секрети.

Відносно асиметричних криптоперетворень криптографічна стійкість до атак «повне розкриття» зводиться до розв’язування математичних задач. Дл перетворень в групі точок еліптичних кривих – до дискретного логарифмування на еліптичній киривій. Ця здача є експодинційно складною.

2. Сутність алгоритму ЕП типу IBS, та його застосування.

Для застосування ЕП IBS-1 та IBS-2 спочатку повинні бути введеними та налаштовані загальні параметри та сгенеровані асиметричні пари ключів. Загальними параметрами ЕП IBS-1 та IBS-2 є:

- U – секретний майстер-ключ – ціле число,

U є [1,q 1];

- V – відкритий майстер-ключ – точка ЕК,

V = [U]P modq , V є G;

- X – особистий (секретний) ключ підписувача – точка ЕК,

X = [U]Y modq , X є G;

- Y – відкритий ключ (перевіряння) підписувача – точка ЕК, Y = H (ID)mod q, Y є G ;

- P – базова точка центру сертифікації ключів порядку q.

Генерація чи обчислення загальних параметрів повинні здійснюватись з дотриманням таких умов: - особистий ключ користувача X обчислюється за його запитом у центрі генерації ключів (ЦГК) та надається користувачеві по захищеному каналу; - відкритий ключ користувача Y може обчислити кожен користувач домену; - ID – є рядок даних, що містить ідентифікатор підписувача;

- H – функція гешування

3. Задача №16.

Визначимо пари ключів ЦГК та підписувача однаковими для IBS-2:

, ; тобто пара ключів ЦГК: (5, (5,19))

, ; тобто пара ключів підписувача: ((13,16), (17,20))

 – ціле повідомлення; розбиваємо його на частини:

IBS-2:  – порожня частина,  – повідомлення, що треба підписати

Вироблення ЕП:

1) , 

2) , 

3) , 

4) , , 

Підписом є .

Перевірка ЕП:

1) , 

2) , 

,



3) , 

Отже, підпис справжній.