**1. Дайте характеристику та обґрунтуйте вимоги до ключової пари для крипто перетворення в групі точок еліптичної кривої**

Розглянемо сутність асиметричних крипто перетворень НШ в групі точок еліптичної кривої.. Також звернемо на крипто перетворення в групі точок еліптичної кривої суттєву увагу, так як перетворення в групі точок витримали випробовування часом, а складність атаки визначення ключа( крипто атаки « повне розкриття) до цих пір носить експоненційний характер.

*Перелік та сутність загальних параметрів*. У 90-х роках було запропоновано використовувати крипто перетворення, що базуються на перетвореннях у групі точок еліптичних кривих над полями F(p), F(2m), F(pm) . **До загальних параметрів еліптичної кривої на полем Галуа F ( Р)** відноситься кортеж

( а, в, G, n, P, u, h) , (2.28)

де:

-  та  параметри еліптичної кривої, які визначають рівняння еліптичної кривої , що використовується ;

-  - базова точка порядку  з координатами  та;

-  порядок базової точки  за умови, що  та  - просте число;

- - розмір поля, який визначає базове кінцеве поле , де  повинно бути, простим числом;

- u =  - порядок еліптичної кривої;

-  коефіцієнт взаємозв’язку порядку кривої  та порядку базової точки , причому .

**До загальних параметрів еліптичної кривої на полем Галуа F ( 2m**) відноситься кортеж

( а, в, G, n, ( f(x), m),u, h) , (2.29)

де:

-  та  параметри еліптичної кривої, які визначають рівняння еліптичної кривої , що використовується ;

-  - базова точка порядку  з координатами  та;

-  базової точки  при умові, що  та  - просте число;

( f(x), m) – примітивний поліном та його степінь;

- u =  - порядок еліптичної кривої;

-  коефіцієнт взаємозв’язку порядку кривої  та порядку базової точки , причому .

Крива, тобто її параметри, ні в якому випадку не повинні вибиратись із переліку значень, що не рекомендуються або заборонені.

**До загальних параметрів еліптичної кривої на полем Галуа F ( рm)** відноситься кортеж

( а, в, G, n, рm ,u, h) , (2.30)

 та  параметри еліптичної кривої, які визначають рівняння еліптичної кривої , що використовується : ;

базова точка  порядку  з координатами  та;

 порядок базової точки  при умові, що  та  - просте число;

 розмір поля, який визначає базове кінцеве поле , де  повинно бути простим числом;

кофактор  взаємозв’язку порядку кривої u та порядку базової точки  причому .

Крива, тобто її параметри, ні в якому випадку не повинні вибиратись із переліку значень, що не рекомендуються або заборонені.

Усі параметри еліптичної кривої повинні генеруватись випадково. Для цього в рекомендується використовувати випадкові бітові рядки SEED. Це відноситься до генерації загальних параметрів еліптичних кривих над скінченними полями. Вибір способів та засобів генерування SEED повинен здійснюватись з урахуванням вимог законодавства(див . розділ 5).

*Генерування асиметричної ключової пари.* Ключова пара

, (3.31)

де:  особистий ключ,  генерується випадково, а відкритий ключ обчислюється засобом виконання скалярного множення, тобто цілого числа та точку еліптичної кривої

, (3.32 )

де G – базова точка на еліптичній кривій порядку n, а QA – відкритий ключ, що є точкою на еліптичній кривій з координатами (ха, уа).

Існує тривимірне подання ЕК, що називається проективною геометрією (базисом). У проективній геометрії кожна точка задається трьома координатами – X, Y, Z.

Основною операцією в групі точок ЕК є скалярне множення вигляду (3.32) для простого поля F(p), а для розширення F(2):

. (3.33)

Стійкість атаки проти загрози повного розкриття визначається складністю розв’язання порівнянь (3.32) і (3.33) відносно особистого ключа d. Складність розв’язування цього рівняння набагато вища, ніж у кільці та полі. У полі – субекспоненційна, а в групі точок еліптичних кривих – експонентна складність.

*Направлене зашифрування блоків інформації*. Нехай мається повідомлення М, розбиваємо його на блоки , довжина яка задовольняє вимоги , тобто менше довжини модуля ln, . Зашифрування здійснюється за правилом

, (3.34)

де:

- k – ключ сеансу (сеансовий);

- - відкритий ключ отримувача.

Також обчислюється відкритий ключ сеансу(зашифрування блоку інформації)

, (3.35)

де G – базова точка на еліптичній кривій.

Далі відправник передає користувачеві одержувачеві два блоки:

- - відкритий ключ сеансу;

-  - блок криптограма.