КРАВЧЕНКО-КБ31

Екзаменаційна робота
з дисципліни прикладна криптологія
студента 3 курсу ФКН групи КБ-31
Кравченка Євгена
Білет №12

① Повне розкриття - противник отримує секретний ключ користувача. Сутність атаки повне розкриття міститься в розв'язку дискретних логарифмічних рівнянь. Якщо криптоаналітик визначить особистий ключ, то в подальшому він зможе нав'язувати хибні загальні секрети та хибні повідомлення. Для суттєвого ускладнення можливості нав'язування хибних загальних секретів використовують як довготривалі, так і сеансові загальні ~~ключі~~ секрети.

Відносно асиметричне криптоперетворень криптографічна стійкість до атак „повне розкриття" зводиться до розв'язання деяких математичних задач. Так, для перетворень в групі точок еліптичних кривих - до дискретного логарифмування на еліптичній кривій. Ця задача є експоненційно складною.

② Для застосування ЕП IBS-1 та IBS-2 спочатку необхідно вибрати та налаштувати загальні параметри та згенерувати асиметричні пари ключів.
Загальними параметрами ЕП є
H - секретний майстер-ключ - ціле число, $H \in [1, q-1]$;
V - відкритий майстер-ключ - точка ЕК, $V = [H]P \bmod q$, $V \in G_1$
X - особистий (секретний) ключ підписувача - точка ЕК, $X = [H]Y \bmod q$, $X \in G_1$
Y - відкритий ключ (перевірки) підписувача - точка ЕК, $Y = H_1(ID) \bmod q$, $Y \in G_1$
P - базова точка центру сертифікації ключів порядку q.

Генерація та обчислення загальних параметрів повинні здійснюватися з дотриманням таких умов:
- особистий ключ користувача X обчислюється за його запитом у ЦГК та передається по захищеному каналу
- ID - рядок, що містить ідентифікатор підписувача
H - ф-я хешування

Нехай ЕП здійснюється з використанням ГОСТ-2, причому використовується крива $y^2 = (x^3 + x + 1) \bmod p$ $p = 23$

Загальні параметри

P - базова точка, $P = (13, 7)$

q - порядок базової точки, $q = 7$

U - секретний майстер-ключ, $U = [1, q-1]$

V - відкритий майстер-ключ, $V = [U] P \bmod q$

x - особистий ключ підписувача, $x = [U] Y \bmod q$

Y - відкритий ключ підписувача, $Y = H_1(ID) \bmod q$

Вирахуємо пари ключів ЦГК та підписувача

$U = 5$, $V = 5 \cdot (13, 7) \bmod q = (5, 19)$, тобто пара ключів ЦГК: $(5, (5, 19))$

$Y = (17, 20)$, $X = 5(17, 20) \bmod q = (13, 16)$, тобто пара ключів підписувача:

$((13, 16), (17, 20))$

Створення ЕП:

1. $K = [1, q-1]$, $K = 6$
2. $\Pi = [K] Y \bmod q$, $\Pi = 6(17, 20) \bmod q = (17, 3)$
3. $R = \Pi$, $R = (17, 3)$
4. $S = [K + H] X \bmod q$, $H = 3$, $S = [6 + 3](13, 16) \bmod q = 2(13, 16) = 5, 19$

Підписом є $\Sigma = (R, S) = ((17, 3), (5, 19))$

Перевірка ЕП

1. $\bar{\Pi} = R$, $\bar{\Pi} = (17, 3)$
2. $\bar{R}_1 = \langle P, S \rangle$, $\bar{R}_1 = \langle (13, 7), (5, 19) \rangle$

   $\bar{R}_2 = \langle V, \bar{\Pi} + [H] Y \rangle$, $\bar{R}_2 = \langle (5, 19), (17, 3) + 3(17, 20) \rangle = \langle (5, 19), (17, 3) + (5, 19) \rangle =$

   $= \langle (5, 19), (13, 7) \rangle$
3. $\bar{R}_1 = \bar{R}_2$, $\langle (13, 7) (5, 19) \rangle = \langle (5, 19), (13, 7) \rangle$

Отже, підпис справжній.