Міністерство освіти і науки України

Харківський національний університет ім. В. Н. Каразіна

Факультет комп’ютерних наук

Кафедра безпеки інформаційних систем і технологій

Лабораторна робота №5

*з навчальної дисципліни*

«Прикладна криптологія»

Виконав:

Студент групи КБ-31 Кравченко Є. М.

Перевірив:

Професор

Горбенко І. Д.

Старший викладач

Єсіна М. В.

Харків – 2020

**Тема лабораторної роботи**

**«Протокол сліпого підпису на основі ISO/IEC 14888-3:2014 (EC-DSA) та ДСТУ 4145-2002»**

**Мета роботи:** Аналіз протоколу сліпого підпису в групі точок еліптичної кривої над простим полем GF(p) на основі алгоритму електронного підпису EC-DSA та ДСТУ 4145-2002.

**Використовуване програмне забезпечення:** програма CrypTool.

**Хід роботи**

Вхідні параметри:

*GF* (23)*, G =* (17, 3), *h =* 2*, n =* 7*, d =* 2*, k =* 3*,* = 5, m = 7

**Протокол сліпого підпису на основі ISO/IEC 14883-3:2014 (EC-DSA)**

* 1. Сліпим підписом під документом  вважається пара значень .

= 2\**G* mod 7 = (13, 16);

=3\**G* mod 7= (5, 4);

 = 2;

= 5\*(5, 4) mod 7 = (17, 3);

=17 mod 7 = 3;

=3 mod 7 = 3;

= 3/3\*2 mod 7 = 2;

= (2\*3+2)/3 mod 7 = 1/3 mod 7 = 5;

* 1. = ((2/5) G+ (3/5) Q) mod 7 = (6\*G + 2\*Q) mod 7 = ((17, 20) + (5, 19)) mod 7= (5, 4) = *E*;
  2. = ((5 \* 1/1)/5) mod 7 = 1;
  3. = ((2 / 1) \* G + (3 / 1) \* Q) mod 7= (13, 16) + (17, 20) mod 7 = (17, 3) = C;

 = 17 mod 7 = 3 = r;

* 1.  = ((5 \* (1/1))/1) mod 7 = 5;

 = 5 \* (5, 4) mod 7 = (17, 3);

 = 17 mod 7 = 3;

**Протокол сліпого підпису на основі ДСТУ 4145-2002**

* 1.  = - 2 \* (17, 3) mod 7 = 5 \*(17, 3) mod 7 = (13, 7);

e = 3

 = 3 \* (17, 3) mod 7 = (5, 4);

 = 2;

 = 5 \* (5, 4) mod 7 = (17, 3);

 = 2 \* 13 mod 7 = 6;

= 3 \* 5 mod 7 = 4;

 = (13 \* 2) / (5 \* 5) mod 7 = 5 / 4 mod 7 = 5;

 = (3 + 2 \* 1) mod 7 = 4;

* 1.  = 5 \* (17, 3) + 1 \* (13, 7) mod 7 = (13,7) + (13, 7) mod 7 = (5, 4) = E;
  2.  = 5 \* 5 mod 7 = 6;
  3.  = 4 \* (17, 3) + 5 \* (13, 7) mod 7 = (5, 19) + (5, 19) mod 7 = (17 ,3);

 = 17 \* 2 mod 7 = 6 = r;

* 1.  = 4 / 5 mod 7 = 5;

 = 5 \* (5, 4) mod 7 = (17, 3);

 = 17 mod 7 = 3;

**Висновки**

У типовій схемі сліпого підпису приймають участь, як правило, три сторони – емітент документу, підписувач та перевіряючий (валідатор).

У випадку сліпого ЕЦП до критеріїв захищеності схеми підпису додається критерій анонімності.

Для перевірки схеми сліпого ЕЦП за критерієм анонімності необхідно з’ясувати, чи може підписувач обчислити підпис у не замаскованому вигляді за допомогою бази даних проміжних значень, яку він створює при постановці підпису.

Розглянувши алгоритми ЕЦП, що базуються на стандарті ISO/IEC 14888-3:2014 (EC-DSA) та ДСТУ 4145-2002, було побудовано на їх основі протокол сліпого електронного підпису. Дослідивши схеми даних сліпих електронних підписів, було визначено, що ці схеми стійкі за критерієм анонімності. Також дослідження цих схем показує, що співвідношення між маскуючими параметрами необхідно обирати таким чином, щоб за ними було неможливо вирахувати автора документу, що ставить підпис під документом.