Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

**Отчет по лабораторной работе №10:**

**«Исследование асимметричных шифров RSA и Эль-Гамаля»**

11 вариант

Студент: Криштопчик А.В.

ФИТ 3 курс 10 группа

Преподаватель: Ржеутская Н.В.

Минск 2023

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.

**Практическая часть**

Задание: разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться доступными библиотеками либо программными кодами.

Реализация:

**script.js**

function RSAInit(randomPrimeNumber1,

randomPrimeNumber2) {

if (typeof randomPrimeNumber1 !== 'number' ||

typeof randomPrimeNumber2 !== 'number') throw new Error('Bad type of params');

if (!isPrimeNumber(randomPrimeNumber1) || !isPrimeNumber(randomPrimeNumber2))

throw new Error('Numbers are not prime');

const n = randomPrimeNumber1 \* randomPrimeNumber2;

const fn = (randomPrimeNumber1 - 1) \* (randomPrimeNumber2 - 1);

const e = 7;

const d = GetNumberByMod(e, fn);

return {

n,

e,

d

};

}

function isPrimeNumber(number) {

for (let i = 2; i < number / 2; ++i)

if (number % i === 0)

return false;

return true;

}

function GetNumberByMod(x, n) {

if (typeof x != 'number' || typeof n != 'number') throw new Error('Bad value type');

if (NOD(x, n) != 1) throw new Error('Числа должна быть взаимно простыми');

let y = 1,

k = 0;

while (true) {

k = (1 - x \* y) / n;

if (Number.isInteger(k))

return y;

else

y++;

}

}

function NOD(a, b) {

if (typeof a != 'number' || typeof b != 'number') throw new Error('Bad type of value');

let max = Math.max(a, b);

let min = Math.min(a, b);

let r = -1;

while (r != 0) {

r = max % min;

max = min;

min = r;

}

return max;

}

function RSA({

n,

e,

d

}, message) {

let crypto = "";

const positionA = 'A'.charCodeAt(0);

for (let i = 0, {

length

} = message; i < length; ++i) {

const alphabetPosition = (message.charCodeAt(i) - positionA) + 1;

crypto += String.fromCharCode((Math.pow(alphabetPosition, e) % n) - 1 + positionA);

}

return crypto;

}

function DecryptRSA({

n,

e,

d

}, message) {

let crypto = "";

const positionA = 'A'.charCodeAt(0);

for (let i = 0, {

length

} = message; i < length; ++i) {

const alphabetPosition = (message.charCodeAt(i) - positionA) + 1;

crypto += String.fromCharCode((Math.pow(alphabetPosition, d) % n) - 1 + positionA);

}

return crypto;

}

//////////////////////////////////////////

function ElGamalInit() {

const [p, g, x] = [11, 2, 8];

const y = Math.pow(g, x) % p;

// console.log ("y =",y);

return {

p,

g,

x,

y

}

}

function ElGamal(keys, message) {

const encrypt = [];

for (let i = 0, {

length

} = message; i < length; ++i) {

encrypt.push(ElGamalSymbol(keys, message[i]));

}

return encrypt;

}

function ElGamalSymbol({

p,

g,

x,

y

}, message) {

const k = Math.round(Math.random() \* (p - 1));

// console.log("k =", k);

const a = Math.pow(g, k) % p;

const b = (Math.pow(y, k) \* message) % p;

return {

a,

b

};

}

function ElGamalDecrypt(keys, message) {

const decrypt = [];

for (let i = 0, {

length

} = message; i < length; ++i) {

decrypt.push(ElGamalSymbolDecrypt(keys, message[i]));

}

return decrypt;

}

function ElGamalSymbolDecrypt({

p,

g,

x,

y

}, {

a,

b

}) {

const m = b \* Math.pow(a, p - x - 1) % p;

return m;

}

const keys = RSAInit(5, 7);

const encryptMessage = RSA(keys, 'ALEKSANDRA, VLADIMIROVNA, KRISHTOPCHIK');

console.log('Зашифрование RSA: ', encryptMessage);

console.log('Расшифрование RSA: ',DecryptRSA(keys, encryptMessage));

const keysElGamal = ElGamalInit();

const encryptElGamal = ElGamal(keysElGamal, [8, 10, 2, 7, 0]);

console.log('Зашифрование Эль-Гамаль: ',encryptElGamal);

console.log('Расшифрование Эль-Гамаль: ',ElGamalDecrypt(keysElGamal, encryptElGamal));

Листинг 1 – Реализация шифров

**Выводы:** приобретены практические навыки асимметричного зашифрования/расшифрования RSA и Эль-Гамаля и разработано соответствующее приложение.