Міністерство освіти та науки України

Національній технічний універсиет України

«Київський політехнічний інститут»

Лабораторна робота № 6

**АСИМЕТРИЧНА**

**КРИПТОСИСТЕМА НА ОСНОВІ МЕТОДУ РЮКЗАКА**

Виконав:

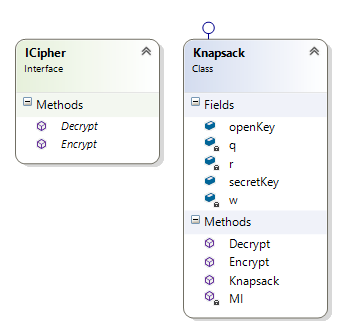
студент 3-го курсу

ТЕФ, групи ТР-21

Самойленко Дмитро

Київ – 2015

Діаграма класів:



Фрагмент функціонального коду:

public string Encrypt(string plainText)

        {

            var bytes = UTF8Encoding.Default.GetBytes(plainText);

            var outBytes = new int[bytes.Length];

            for (int i = 0; i < bytes.Length; i++)

            {

                int sum = 0;

                int c = bytes[i];

                for (int j = openKey.Length - 1; j >= 0; j--)

                {

                    sum += openKey[j] \* (c & 1);

                    c = c >> 1;

                }

                outBytes[i] = sum;

            }

            var output = new StringBuilder();

            foreach (var b in outBytes)

                output.Append(b + " ");

            return  output.ToString();

        }

        public string Decrypt(string cryptedText)

        {

            if (secretKey == null)

                throw new Exception("No secret key!");

            var parts = cryptedText.Split(' ').Select(Int32.Parse).ToList();

            var output  = new StringBuilder(parts.Count);

            var inverse = MI(r, q);

            for (int i = 0; i < parts.Count; i++)

            {

                var m = parts[i] \* inverse % q;

                var ans = 0;

                for (int j = secretKey.Length - 1; j >= 0; j--)

                {

                    ans <<= 1;

                    if (m >= secretKey[j])

                    {

                        m -= secretKey[j];

                        ans |= 1;

                    }

                }

                var symbols = (Convert.ToString(ans, 2)).

PadLeft(secretKey.Length, '0').

ToCharArray();

                Array.Reverse(symbols);

                ans = Convert.ToInt32(new String(symbols), 2);

                char a = Convert.ToChar(ans);

                output.Append(a);

            }

            return output.ToString();

        }

Конструктор класу:

public Knapsack(int[] openKey, int w, Int32 q, Int32 r)

        {

            this.openKey = new int[openKey.Length];

            Array.Copy(openKey, this.openKey, openKey.Length);

            this.w = w;

            this.r = r;

            this.q = q;

        }

        private Int32 MI(int value, int mod)

        {

            for (int i = 0; i <= mod; i++)

            {

                if ((value \* i) % mod == 1)

                    return i;

            }

            return -1;

        }