Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»
Кафедра информатики

Отчет по лабораторной работе №2

Идентификация и аутентификация пользователей. Протокол Kerberos

Выполнил: Студент гр. 853503
Яговдик О.И.

Проверил: Протько М.И.

Минск 2021

Введение

Целью данной лабораторной было реализовать программные средства протокола распределения ключей Kerberos вместе с процедурой, которая реализует Алгоритм DES. ЗАДАНИЕ: 1) Изучить теоретические сведения. 2) Создать приложение, реализующее протокол распределения ключей Kerberos, включая процедуру, реализующую Алгоритм DES. В интерфейсе приложения должны быть наглядно представлены: – Исходные данные протокола (модули, ключи, секретные данные и т.п.); – Данные, передаваемые по сети каждой из сторон; – Проверки, выполняемые каждым из участников. Процесс взаимодействия между сторонами протокола может быть реализован при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Протокол Kerberos

Протокол Kerberos является одной из реализаций протокола аутентификации с использованием третьей стороны, призванной уменьшить количество сообщений, которыми обмениваются стороны.

Протокол Kerberos, достаточно гибкий и имеющий возможности тонкой настройки под конкретные применения, существует в нескольких версиях. Мы рассмотрим упрощенный механизм аутентификации, реализованный с помощью протокола Kerberos версии 5 (рис. 1):

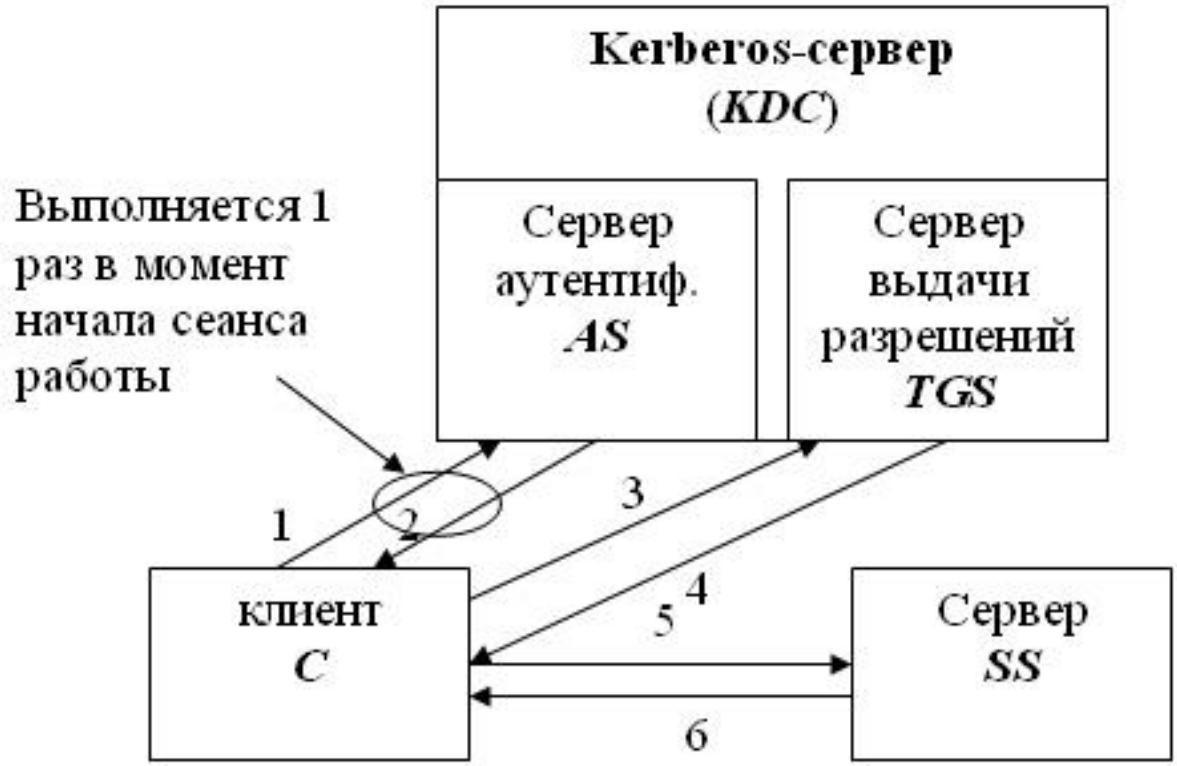


Рисунок 1 Схема протокола Kerberos

Прежде всего стоит сказать, что при использовании Kerberos нельзя напрямую получить доступ к какому-либо целевому серверу. Чтобы запустить собственно процедуру аутентификации, необходимо обратиться к специальному серверу аутентификации с запросом, содержащим логин пользователя. Если сервер не находит автора запроса в своей базе данных, запрос отклоняется. В противном случае сервер аутентификации работает по следующему рабочему процессу:

Рабочий этап:

Пусть клиент C собирается начать взаимодействие с сервером SS (англ. *Service Server* - *сервер*, предоставляющий сетевые сервисы). В несколько упрощенном виде, протокол предполагает следующие шаги:

1. C->AS: {c}.

Клиент C посылает серверу аутентификации AS свой идентификатор c (идентификатор передается открытым текстом).

2. AS->C: {{TGT}K_{AS_TGS}, K_{C_TGS}}K_C,

где:

- K_C - основной ключ C ;
- K_{C_TGS} - ключ, выдаваемый C для доступа к серверу выдачи разрешений *TGS* ;
- {TGT} - *Ticket* Granting *Ticket* - билет на доступ к серверу выдачи разрешений

{TGT}={c,*tgs*,t_1,p_1, K_{C_TGS}}, где *tgs* - идентификатор сервера выдачи разрешений, t_1 - отметка времени, p_1 - *период действия* билета.

Запись $\{\cdot\}K_X$ здесь и далее означает, что содержимое фигурных скобок зашифровано на ключе K_X (Алгоритм шифрования приводится ниже).

На этом шаге сервер аутентификации AS, проверив, что клиент C имеется в его базе, возвращает ему билет для доступа к серверу выдачи разрешений и ключ для взаимодействия с сервером выдачи разрешений. Вся посылка зашифрована на ключе клиента C. Таким образом, даже если на первом шаге взаимодействия идентификатор c послал не клиент C, а нарушитель X, то полученную от AS посылку X расшифровать не сможет.

Получить доступ к содержимому билета TGT не может не только нарушитель, но и клиент C, т.к. билет зашифрован на ключе, который распределили между собой сервер аутентификации и сервер выдачи разрешений.

3. C->*TGS*: {TGT}K_{AS_TGS}, {Aut_1} K_{C_TGS}, {ID}

где {Aut_1} - аутентификационный блок - Aut_1 = {c,t_2}, t_2 - метка времени; ID - идентификатор запрашиваемого сервиса (в частности, это может быть идентификатор сервера SS).

Клиент C на этот раз обращается к серверу выдачи разрешений TGS. Он пересылает полученный от AS билет, зашифрованный на ключе K_{AS_TGS}, и аутентификационный блок, содержащий идентификатор c и метку времени, показывающую, когда была сформирована посылка. Сервер выдачи разрешений расшифровывает билет TGT и получает из него информацию о том, кому был выдан билет, когда и на какой срок, ключ шифрования, сгенерированный сервером AS для взаимодействия между клиентом C и сервером *TGS*. С помощью этого ключа расшифровывается аутентификационный блок. Если метка в блоке совпадает с меткой в билете, это доказывает, что посылку сгенерировал на самом деле C (ведь только он

знал ключ K_{C_TGS} и мог правильно зашифровать свой идентификатор). Далее делается проверка времени действия билета и времени отправления посылки **3**). Если проверка проходит и действующая в системе политика позволяет клиенту C обращаться к клиенту SS, тогда выполняется шаг **4**).

4. *TGS*->C: {{*TGS*}K_{TGS_SS},K_{C_SS}}K_{C_TGS},

где K_{C_SS} - ключ для взаимодействия C и SS, {*TGS*} - *Ticket* Granting Service - билет для доступа к SS (обратите внимание, что такой же аббревиатурой в описании протокола обозначается и сервер выдачи разрешений). {*TGS*} ={c,ss,t_3,p_2, K_{C_SS} }.

Сейчас сервер выдачи разрешений *TGS* посылает клиенту C ключ шифрования и билет, необходимые для доступа к серверу SS. Структура билета такая же, как на шаге 2): идентификатор того, кому выдали билет; идентификатор того, для кого выдали билет; отметка времени; *период действия*; ключ шифрования.

5. C->SS: {*TGS*}K_{TGS_SS}, {Aut_2} K_{C_SS}

где Aut_2={c,t_4}.

Клиент C посылает билет, полученный от сервера выдачи разрешений, и свой аутентификационный блок серверу SS, с которым хочет установить сеанс защищенного взаимодействия. Предполагается, что SS уже зарегистрировался в системе и распределил с сервером *TGS* ключ шифрования K_{TGS_SS}. Имея этот ключ, он может расшифровать билет, получить ключ шифрования K_{C_SS} и проверить подлинность *отправителя сообщения*.

6. SS->C: {t_4+1}K_{C_SS}

Смысл последнего шага заключается в том, что теперь уже SS должен доказать C свою подлинность. Он может сделать это, показав, что правильно расшифровал предыдущее сообщение. Вот поэтому, SS берет отметку времени из аутентификационного блока C, изменяет ее заранее определенным образом (увеличивает на 1), шифрует на ключе K_{C_SS} и возвращает C.

Если все шаги выполнены правильно и все проверки прошли успешно, то стороны взаимодействия C и SS, во-первых, удостоверились в подлинности друг друга, а во-вторых, получили *ключ* шифрования для защиты сеанса связи - *ключ* K_{C_SS}.

Нужно отметить, что в процессе сеанса работы клиент проходит шаги 1) и 2) только один раз. Когда нужно получить билет на *доступ* к другому серверу (назовем его SS1), клиент C обращается к серверу выдачи разрешений *TGS* с уже имеющимся у него билетом, т.е. протокол выполняется начиная с шага 3).

В алгоритме Kerberos могут применяться различные алгоритмы блочного симметричного шифрования. Для целей настоящей работы будем использовать алгоритм DES:

Алгоритм DES Основные сведения

Одной из наиболее известных криптографических систем с закрытым ключом является DES – Data Encryption Standard. Эта система первой получила статус государственного стандарта в области шифрования данных. Она

разработана специалистами фирмы IBM и вступила в действие в США 1977 году. Алгоритм DES по-прежнему широко применяется и заслуживает внимания при изучении блочных шифров с закрытым ключом.

Стандарт DES построен на комбинированном использовании перестановки, замены и гаммирования. Шифруемые данные должны быть представлены в двоичном виде.

DES является классической *сетью Фейстеля* с двумя ветвями. Данные шифруются 64-битными блоками, используя 56-битный ключ. Алгоритм преобразует за несколько *раундов* 64-битный вход в 64-битный выход. Длина ключа равна 56 битам. Процесс шифрования состоит из четырех этапов. На первом из них выполняется начальная перестановка (*IP*) 64-битного исходного текста (забеливание), во время которой биты переупорядочиваются в соответствии со стандартной таблицей. Следующий этап состоит из 16 *раундов* одной и той же функции, которая использует операции сдвига и подстановки. На третьем этапе левая и правая половины выхода последней (16-й) итерации меняются местами. Наконец, на четвертом этапе выполняется перестановка IP^{-1} результата, полученного на третьем этапе. Перестановка IP^{-1} инверсна начальной перестановке.

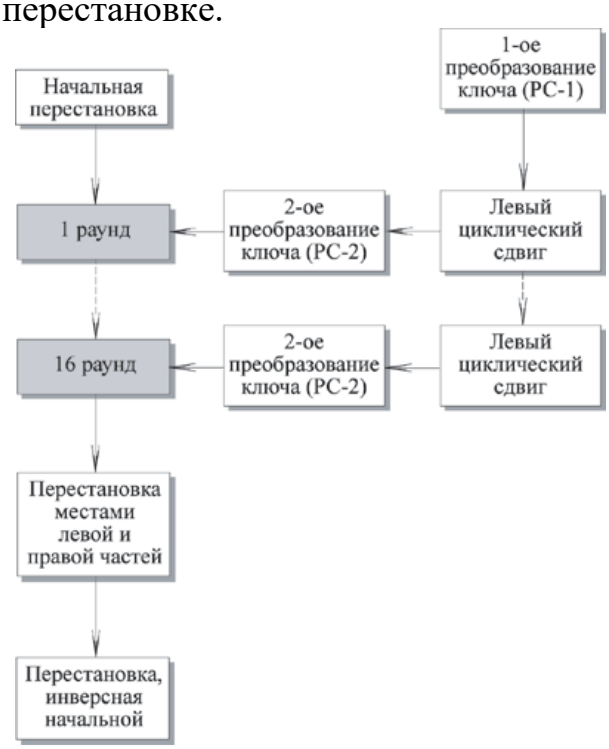


Рисунок 2 Общая схема DES

Шифрование

Начальная перестановка

Начальная перестановка и ее инверсия определяются стандартной таблицей. Если M- это произвольные 64 бита, то X = IP (M)-переставленные 64 бита. Если применить обратную функцию перестановки $Y = IP^{-1}(X) = IP^{-1}(IP(M))$, то получится первоначальная последовательность бит.

Последовательность преобразований отдельного раунда

Теперь рассмотрим последовательность преобразований, используемую в каждом *раунде*.

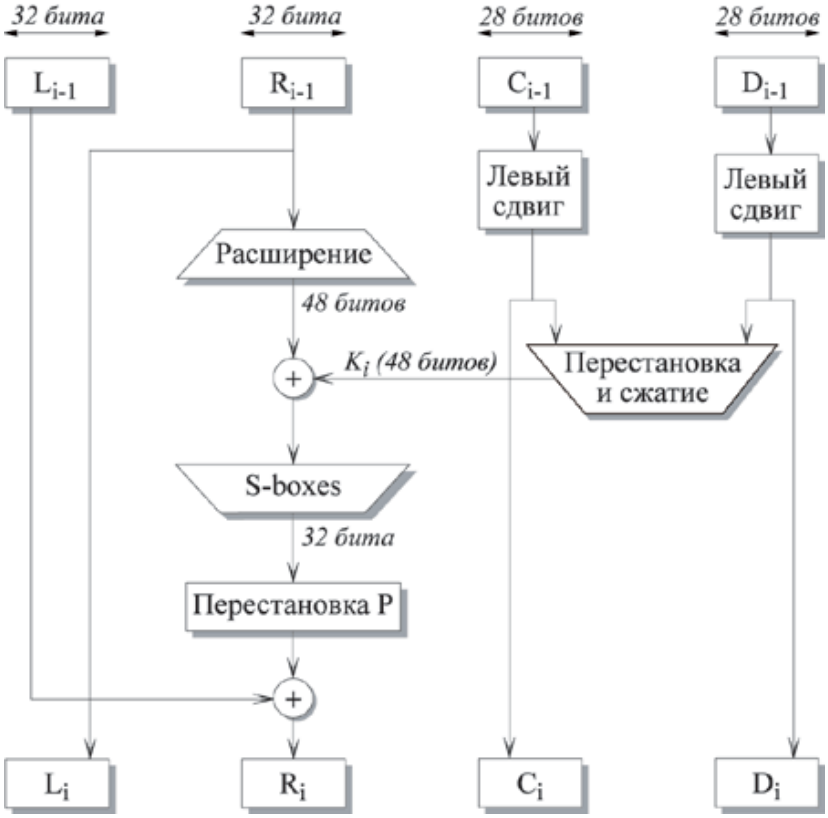


Рисунок 3 - I-ый раунд DES

64-битный входной блок проходит через 16 *раундов*, при этом на каждой итерации получается промежуточное 64-битное значение. Левая и правая части каждого промежуточного значения трактуются как отдельные 32-битные значения, обозначенные L и R. Каждую итерацию можно описать следующим образом:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

Где $\oplus$ обозначает операцию XOR.

Таким образом, выход левой половины L_i равен входу правой половины R_{i-1}. Выход правой половины R_i является результатом применения операции XOR к L_{i-1} и функции F, зависящей от R_{i-1} и K_i.

Рассмотрим функцию F более подробно.

R_i, которое подается на вход функции F, имеет длину 32 бита. Вначале R_i расширяется до 48 бит, используя таблицу, которая определяет перестановку плюс расширение на 16 бит. Расширение происходит следующим образом. 32 бита разбиваются на группы по 4 бита и затем расширяются до 6 бит, присоединяя крайние биты из двух соседних групп. Например, если часть входного сообщения

. . . efgh ijkl mnop . . .

то в результате расширения получается сообщение

. . . defghi hijklm lmnopq . . .

После этого для полученного 48-битного значения выполняется операция XOR с 48-битным *подключом* K_i. Затем полученное 48-битное значение подается на вход функции подстановки, результатом которой является 32-битное значение.

Подстановка состоит из восьми *S-boxes*, каждый из которых на входе получает 6 бит, а на выходе создает 4 бита. Эти преобразования определяются специальными таблицами. Первый и последний биты входного значения *S-box* определяют номер строки в таблице, средние 4 бита определяют номер столбца. Пересечение строки и столбца определяет 4-битный выход. Например, если входом является 011011, то номер строки равен 01 (строка 1) и номер столбца равен 1101 (столбец 13). Значение в строке 1 и столбце 13 равно 5, т.е. выходом является 0101.

שורה	מס' עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	S_5															
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	S_6															
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	S_7															
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Рисунок 4 - S-boxes

Далее полученное 32-битное значение обрабатывается с помощью перестановки *P*, целью которой является максимальное переупорядочивание бит, чтобы в следующем *раунде* шифрования с большой вероятностью каждый бит обрабатывался другим *S-box*.

Создание подключей

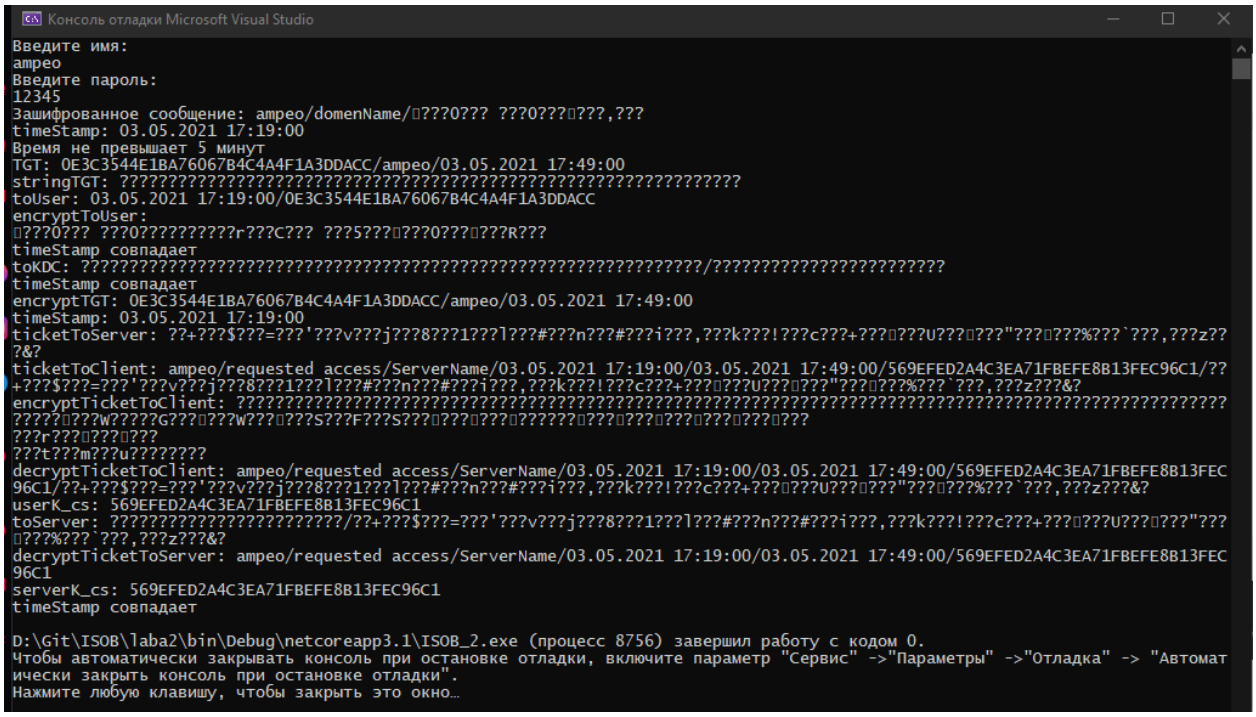
Ключ для отдельного *раунда* K_i состоит из 48 бит. Ключи K_i получаются по следующему алгоритму. Для 56-битного ключа, используемого на входе алгоритма, вначале выполняется перестановка в соответствии с таблицей Permuted Choice 1 (PC-1). Полученный 56-битный ключ разделяется на две 28-битные части, обозначаемые как C_0 и D_0 соответственно. На каждом *раунде* C_i

и D_i независимо циклически сдвигаются влево на 1 или 2 бита, в зависимости от номера *раунда*. Полученные значения являются входом следующего *раунда*. Они также представляют собой вход в Permuted Choice 2 (PC-2), который создает 48-битное выходное значение, являющееся входом функции $F(R_{i-1}, K_i)$.

Дешифрование

Процесс дешифрования аналогичен процессу шифрования. На входе алгоритма используется зашифрованный текст, но ключи K_i используются в обратной последовательности. K_{16} используется на первом *раунде*, K_1 используется на последнем *раунде*.

Результат выполнения



Выводы

DES был национальным стандартом США в 1977—1980 гг., но в настоящее время DES используется (с ключом длины 56 бит) только для устаревших систем, чаще всего используют его более криптоустойчивый вид (3DES, DESX). 3DES является простой эффективной заменой DES, и сейчас он рассмотрен как стандарт. В ближайшее время DES и Triple DES будут заменены алгоритмом AES (Advanced Encryption Standard — Расширенный Стандарт Шифрования). Kerberos является одним из самых распространенных протоколов аунтефикации. В настоящее время множество ОС поддерживают данный протокол, в число которых входят: Windows 2000 и более поздние версии, которые используют Kerberos как метод аутентификации в домене между участниками, различные UNIX и UNIX подобные ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD, Solaris, AIX, OpenVMS).

Код программы

```
using System;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Security.Cryptography;
using System.Text;
using System.Threading;
using System.Collections.Generic;

namespace ISOB_2_Client
{
    class Program
    {
        static void Main(string[] args)
        {
            string domenName = "domenName";
            Console.WriteLine("Введите имя:");
            string userName = Console.ReadLine();
            Console.WriteLine("Введите пароль:");
            string password = Console.ReadLine();
            User clientUser = new User(userName, password);

            var value = new StringBuilder();
            value.Append(userName + "/");
            value.Append(domenName + "/");
            var userTime = DateTime.Now;
            value.Append(new DES().Encrypt(userTime.ToString(),
clientUser.PasswordHash));
            string message = value.ToString();

            Console.WriteLine($"Зашифрованное сообщение: { message }");


            var userList = new Dictionary<string, string>();
            userList.Add("ampeo", "12345");

            DateTime timeStamp;
            User KDKuser ;

            if (userList.ContainsKey(message.Split('/')[0]))
            {
                KDKuser = new User(message.Split('/')[0],
userList[message.Split('/')[0]]);
                timeStamp = DateTime.Parse(new
DES().Decipher(message.Split('/')[2], KDKuser.PasswordHash));
                if (timeStamp.AddMinutes(5) > DateTime.Now)
                {
                    Console.WriteLine("timeStamp: " + timeStamp);
                    Console.WriteLine("Время не превышает 5 минут");
                }
                else
                {
                    Console.WriteLine("Время превышает 5 минут");
                    Console.ReadLine();
                    return;
                }
            }
            else
```

```
            {
                Console.WriteLine("Пользователь не найден");
                Console.ReadLine();
                return;
            }



            string KDCsessionKey = GetHash(new Random().Next(1000000,
9999999).ToString());
            string KDCMasterKey = GetHash("masterKey");
            var TGT = new StringBuilder();
            TGT.Append(KDCsessionKey + "/");
            TGT.Append(KDKuser.Name + "/");
            TGT.Append(DateTime.Now.AddMinutes(30).ToString());
            string encryptTGT = new DES().Encrypt(TGT.ToString(),
KDCMasterKey);
            Console.WriteLine("TGT: " + TGT);
            Console.WriteLine("stringTGT: " + encryptTGT);



            var toUser = new StringBuilder();
            toUser.Append(timeStamp + "/");
            toUser.Append(KDCsessionKey);
            string encryptToUser = new DES().Encrypt(toUser.ToString(),
KDKuser.PasswordHash);
            Console.WriteLine("toUser: " + toUser);
            Console.WriteLine("encryptToUser: ");
            Console.WriteLine(encryptToUser);

            string decryptToUser = new DES().Decipher(encryptToUser,
clientUser.PasswordHash);
            timeStamp = DateTime.Parse(decryptToUser.Split('/')[0]);
            string userSessionKey;
            if (timeStamp.ToString().Equals(userTime.ToString()))
            {
                userSessionKey = decryptToUser.Split('/')[1];
                Console.WriteLine("timeStamp совпадает");
            }
            else
            {
                Console.WriteLine("timeStamp не совпадает");
                Console.ReadLine();
                return;
            }

            var toKDC = new StringBuilder();
            toKDC.Append(encryptTGT + "/");
            userTime = DateTime.Now;
            toKDC.Append(new DES().Encrypt(userTime.ToString(),
userSessionKey));
            Console.WriteLine("toKDC: " + toKDC);

            encryptTGT = new
DES().Decipher(toKDC.ToString().Split('/')[0], KDCMasterKey);
            timeStamp = DateTime.Parse(new
DES().Decipher(toKDC.ToString().Split('/')[1], KDCsessionKey));
            if (timeStamp.AddMinutes(5) > DateTime.Now)
            {
                Console.WriteLine("timeStamp совпадает");
```

```
                Console.WriteLine("encryptTGT: " + encryptTGT);
                Console.WriteLine("timeStamp: " + timeStamp);
            }
            else
            {
                Console.WriteLine("timeStamp не совпадает");
                Console.ReadLine();
                return;
            }

            var ticketToClient = new StringBuilder();
            ticketToClient.Append(KDKuser.Name + "/");
            ticketToClient.Append("requested access" + "/");
            ticketToClient.Append("ServerName" + "/");
            ticketToClient.Append(DateTime.Now + "/");
            ticketToClient.Append(DateTime.Now.AddMinutes(30) + "/");
            string keyK_cs = GetHash("keyK_cs" + "/");
            ticketToClient.Append(keyK_cs);
            string serverMasterKey =  GetHash("serverMasterKey");
            var ticketToServer = new
DES().Encrypt(ticketToClient.ToString(), serverMasterKey);
            ticketToClient.Append("/" + ticketToServer);
            Console.WriteLine("ticketToServer: " + ticketToServer);
            Console.WriteLine("ticketToClient: " + ticketToClient);


            var encryptTicketToClient = new
DES().Encrypt(ticketToClient.ToString(), KDCsessionKey);
            Console.WriteLine("encryptTicketToClient: " +
encryptTicketToClient);


            var decryptTicketToClient = new
DES().Decipher(encryptTicketToClient, userSessionKey);
            Console.WriteLine("decryptTicketToClient: " +
decryptTicketToClient);
            var userK_cs = decryptTicketToClient.Split('/')[5];
            Console.WriteLine("userK_cs: " + userK_cs);

            var toServer = new StringBuilder();
            toServer.Append(new DES().Encrypt(DateTime.Now.ToString(),
userK_cs));
            toServer.Append("/" + decryptTicketToClient.Split('/')[6]);

            Console.WriteLine("toServer: " + toServer);


            var decryptTicketToServer = new
DES().Decipher(toServer.ToString().Split("/")[1], serverMasterKey);
            Console.WriteLine("decryptTicketToServer: " +
decryptTicketToServer);
            var serverK_cs = decryptTicketToServer.Split("/")[5];
            Console.WriteLine("serverK_cs: " + serverK_cs);
            if (DateTime.Parse(new
DES().Decipher(toServer.ToString().Split("/")[0],
serverK_cs)).AddMinutes(5) > DateTime.Now)
            {
                Console.WriteLine("timeStamp совпадает");
            }
            else
            {
```

```
                Console.WriteLine("timeStamp не совпадает");
                Console.ReadLine();
                return;
            }
        }

        private static string GetHash(string str)
        {
            var tmpSource = ASCIIEncoding.ASCII.GetBytes(str);
            var tmpHash = new
MD5CryptoServiceProvider().ComputeHash(tmpSource);
            StringBuilder value = new StringBuilder(tmpHash.Length);
            for (int i = 0; i < tmpHash.Length; i++)
            {
                value.Append(tmpHash[i].ToString("X2"));
            }
            return value.ToString();
        }
    }
}
```