Вариант 03

Курсовая работа «Шифрование в сетях 802.11»

Задание 1:

1. Исходные данные для всех вариантов:

a.   Метод аутентификации PSK.

b. Название сети SSID: sibsutis

c.   MAC-адрес точки доступа(шестн.): 000726404eff

d. MAC-адрес клиента (шестн.): 9439e5b014e5

2. Пароль к Wi-Fi сети: kursovikXY, где XY –ваш вариант.

3. Сгенерировать самостоятельно (придумать) последовательности Anonce и Snonce таким образом, чтобы первый и последний байт был равен вашему варианту, т.е. XY.

4. Вычислить ключ PTK и разделить его на части KEK, KCK и TK.

a.   Если XY четное – расчет PTK делается для шифрования CCMP.

b. Если XY нечетное – расчет PTK делается для шифрования TKIP.

5. Сгенерировать групповой ключ GTK самостоятельно (придумать) таким образом, чтобы первый и последний байт был равен вашему варианту, т.е. XY.

6. В шестнадцатеричном виде сконструировать четыре (т.е. все) передаваемые EAPOL-Key кадры в процессе четырехкратного рукопожатия. Изобразить их в виде четырех таблиц следующим образом:

|  |  |  |
| --- | --- | --- |
| Название поля кадра | Размер поля в байтах или битах | Значение поля в шестнадцатеричном виде |
|   |   |   |

Поле Key Data шифровать не нужно! Соответственно оставьте поле EAPOL-Key IV нулевым.

Задание 2

Изобразить и пояснить схему процесса шифрования с указанием известных или вычисленных в задании 1 данных (PTK, MAC-адреса и т.д.)

Примеры приведены в курсе лекций.

**Список рекомендуемой литературы**

**Рекомендуемая литература**

*Список основной литературы*

1.      Заика А.А. Локальные сети и интернет [Электронный ресурс]/ Заика А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 323 c.— Режим доступа: http://www.iprbookshop.ru/52150.html.— ЭБС «IPRbooks»

2.     Беспроводные сети Wi-Fi [Электронный ресурс]/ А.В. Пролетарский [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 284 c.— Режим доступа: http://www.iprbookshop.ru/52183.html.— ЭБС «IPRbooks»

3.     Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

*Список дополнительной литературы*

1.      Носкова Н.В. Стандарты беспроводных телекоммуникационных сетей [Электронный ресурс]: учебное пособие/ Носкова Н.В.— Электрон. текстовые данные.— Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2012.— 201 c.— Режим доступа: http://www.iprbookshop.ru/45489.html.— ЭБС «IPRbooks

2.      Кокорева Е.В. Основы беспроводной связи [Электронный ресурс]: учебно-методическое пособие/ Кокорева Е.В., Белезекова А.С.— Электрон. текстовые данные.— Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2015.— 70 c.— Режим доступа: http://www.iprbookshop.ru/55489.html.— ЭБС «IPRbooks»

*Информационное обеспечение*

1.      Максим Мерритт Безопасность беспроводных сетей [Электронный ресурс]/ Максим Мерритт, Дэвид Поллино— Электрон. текстовые данные.— М.: ДМК Пресс, 2008.— 288 c.— Режим доступа: http://www.iprbookshop.ru/7852.— ЭБС «IPRbooks», по паролю

2.      Берлин А.Н. Сотовые системы связи [Электронный ресурс]/ Берлин А.Н.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 430 c.— Режим доступа: http://www.iprbookshop.ru/52177.html.— ЭБС «IPRbooks»

3.      Алексеев В.А. Беспроводные локальные сети IEEE 802.11 Wi-Fi [Электронный ресурс]: методические указания к проведению лабораторных работ по курсу «Сети ЭВМ и телекоммуникации»/ Алексеев В.А.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2012.— 26 c.— Режим доступа: http://www.iprbookshop.ru/17720.html.— ЭБС «IPRbooks»

***Электронные ресурсы и источники на английском:***

1. Стандарт «IEEE 802.11™-2012». Для скачивания надо ввести эл. почту и выбрать тип пользователя.
<http://standards.ieee.org/getieee802/download/802.11-2012.pdf>
2. Jeremy Quirke «Security in the GSM system»
[http://nashville.dyndns.org:823/YourFreeLibrary/Encryption%20And%20Security/Security+in+the+GSM+system+01052004.pdf](http://nashville.dyndns.org:823/YourFreeLibrary/Encryption%20And%20Security/Security%2Bin%2Bthe%2BGSM%2Bsystem%2B01052004.pdf)
3. Kevin Benton «The Evolution of 802.11 Wireless Security»
<http://homes.soic.indiana.edu/ktbenton/research/benton_wireless.pdf>
4. Спецификация на все открытые алгоритмы на портале 3GPP.
<http://www.3gpp.org/Confidentiality-Algorithms>.