КМЗИ – Упражнение No9

Задачи:

1. Разгледайте демонстрационния пример на:
http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf

2. Попълнете следната сравнителна таблица

	DES	**AES**
Разработен (година)	1977	1998
Утвърден стандарт (година)	1981	2002
Автор	Разработен от IBM и базиран на по-ранен дизайн от Хорст Фейстел	Винсент Реймен и Жоан Дамен
Дължина на ключа	56 бита	128, 192 или 256 бита
Вид на алгоритъма	Симетричен ключов алгоритъм за криптиране на цифрови данни	Алгоритъм със симетричен ключ, което означава, че един и същ ключ се използва както за криптиране електронни данни, така и за дешифриране на данните.
Размер на блока	64 бита	128 бита
Алгоритми, които използва	DES шифърът е производен на Lucifer шифър.	Rijndael
Брой на рундовете	16 рунда	10, 12, 14 рунда
Предимства	Шифроването и декриптирането имат един и същ алгоритъм. 56 - битов ключ - има 2 ^ 56 възможни клавишни комбинации, които биха отнели десетилетие, за да се намери правилният ключ, използвайки силова атака.	Шифърът е напълно самостоятелен – той не използва никакви части заимствани от други шифри, има отчетлива и ясна структура, тоест неговата устойчивост не се основава на някакви сложни и не напълно разбираеми преобразувания.
Недостатъци	Базовият алгоритъм DES е загубил значимостта си като стандарт, най-вече заради недостатъчната си дължина на ключа от 56 бита и уязвимостта от диференциален и линеен криптоанал Два избрани входа към S-кутия могат да създадат един и същ изход.	Режимът на разшифриране се различава от режима на шифриране не само заради последователността на функциите, но и самите функции се различават със своите параметри от използваните в режима на шифриране. Този факт се отразява на ефективността на апаратната реализация на шифъра.
Защита	Доказано неадекватна	Смята се за надеждна

3. Представете поне 3 приложения на AES стандарта.

    1. **ИНСТРУМЕНТИ ЗА АРХИВИРАНЕ И КОМПРЕСИРАНЕ**
    2. **ШИФРОВАНЕ НА ДИСК / ДЯЛ**
    3. **ВИРТУАЛНИ ЧАСТНИ МРЕЖИ(VPN)**
    4. **ЗА ИЗПРАЩАНЕ НА СЪОБЩЕНИЯ ПРЕЗ WhatsApp или Facebook Messenger… - AES algorithm.**

4. Разгледайте примерни програмни реализации на AES на:
https://gist.github.com/bricef/2436364
http://stackoverflow.com/questions/15554296/simple-java-aes-encrypt-decrypt-example
http://aesencryption.net/
http://aes.online-domain-tools.com/
http://testprotect.com/appendix/AEScalc