16.03.2024

Курс:

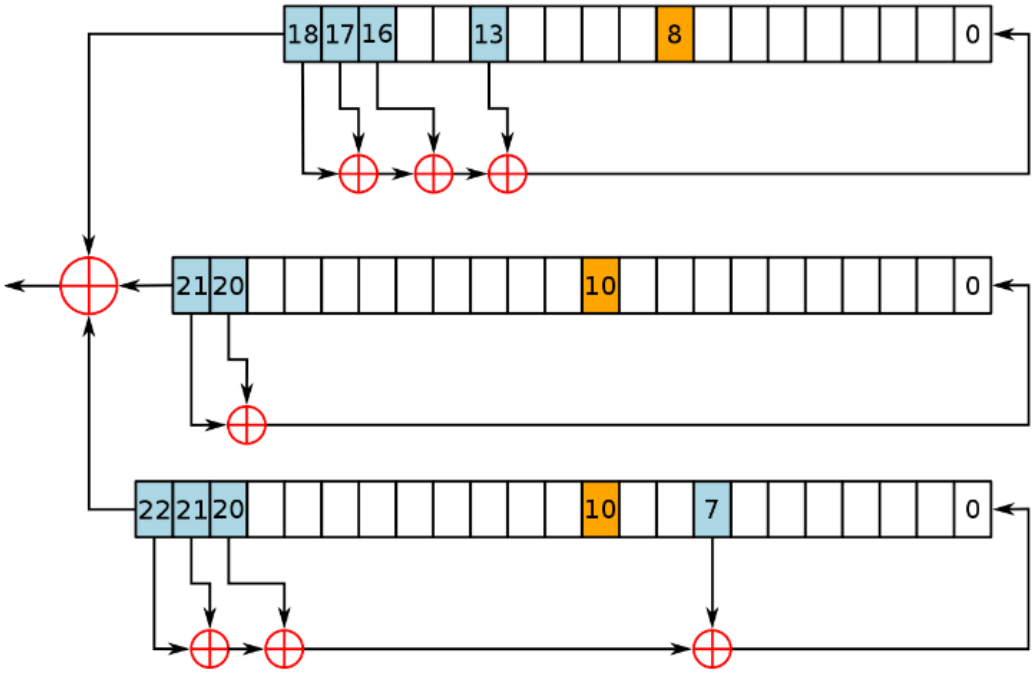
Практическая работа к уроку № Lesson_5

--

Асимметричная криптография и другие темы

Асимметричная криптография - криптосистема, в которой шифрование и дешифрование происходит с помощью пары разных ключей (открытый и закрытый).
Асимметричная криптография — криптосистема, в которой шифрование и дешифрование происходит с помощью пары разных ключей открытый и закрытый).
Шифрование RSA Для шифрования с помощью RSA используется открытый ключ, а для расшифрования используется закрытый ключ.
Подпись RSA Для подписи с помощью RSA используется закрытый ключ, а для проверки подписи используется открытый ключ.
Симметрия vs асимметрия Главная причина, по которой асимметричная криптография не заменила симметричную — скорость вычислений.
Проблему обмена симметричными ключами шифрования можно решить с помощью RSA.
Алгоритм **Диффи-Хеллмана** позволяет установить ключ шифрования при передаче данных по публичному каналу.

Потоковые шифры



Задание_1:

В этом задании вам необходимо “расшифровать” 4 “шифротекста”:

```
SXQncyBiYXNlNjQK
497473206120686578
SGksIE1hcmlhLiBIb3cgYXJlIHlvdT8K
KVXGK6DQMVRXIZLEEBSW4Y3PMRUW4ZZOEBBHK5BAPFXXKIDENFSCA2LUFQQHE2LHNB
2D6CQ=
```

```
#include "_XOR.au3"
$xor = _Xor_Encode("TEST_TEXT", 25)
$unxor = _Xor_Decode($xor, 25)
MsgBox(64, "", "Encoded: "& $xor &@CRLF&@CRLF&"Decoded: "& $unxor)


; _XOR.au3
#include "Array.au3"
; #FUNCTION# ====================================
; Name...........: _Xor_Encode
; Author.........: []
; ===============================================

Func _Xor_Encode($sString, $iKey = 25)
        $sString2 = String($sString)
```

```
        $StrLen = StringLen($sString2)
        $Array = StringToASCIIArray($sString2)
        Dim $Chr[StringLen($sString2)]

        For $i = 0 To $StrLen - 1 Step 1
                $Array[$i] = BitXOR($Array[$i], $iKey)
        Next

        For $i = 0 To $StrLen - 1 Step 1
                $Chr[$i] = ChrW($Array[$i])
        Next

        Return _ArrayToString($Chr, "")
EndFunc

; #FUNCTION# ====================================
; Name...........: _Xor_Decode
; Author.........: []
; ================================================

Func _Xor_Decode($sString, $iKey = 25)
        $sString2 = String($sString)
        $StrLen = StringLen($sString2)
        $Array = StringToASCIIArray($sString2)
        Dim $Chr[StringLen($sString2)]

        For $i = 0 To $StrLen - 1 Step 1
                $Chr[$i] = BitXOR($Array[$i], $iKey)
        Next

        For $i = 0 To $StrLen - 1 Step 1
                $Chr[$i] = ChrW($Chr[$i])
        Next

        Return _ArrayToString($Chr, "")
EndFunc
```

```autoit
$iRendom = Random(1, 255, 1)

$En_Xor = __xor_Crypt('Обычная строка (The usual line of)',
$iRendom)
```

```
$Un_Xor = __xor_Crypt($En_Xor, $iRendom)

MsgBox(64, 'Result', 'Encoded: ' & @CRLF & $En_Xor & @CRLF & @CRLF
& 'Decoded: ' & @CRLF & $Un_Xor)

Func __xor_Crypt($sString, $iKey = 70)
        Local $sRet, $aAscii =
StringToASCIIArray(String($sString))
    If ($iKey == 0) Then Return SetError(1, 0, 0)
    For $i = 0 To UBound($aAscii) -1
            $sRet &= ChrW(BitXOR($aAscii[$i], $iKey))
    Next
        Return SetError(0, $iKey, $sRet)
EndFunc
```

Задание 2

Ниже представлены хеши некоторых словарных паролей. Найдите их исходные значения (сами пароли).

```
8cca64749f22aa0c1925c2e21e452f4fd33b0ce11d9dc9a5cabd244458f34089
2ddf70ab0eed47a05a45bfc44707dfad
512c3550c043c07d4419bcf4bcd5bdab748d4586
e12bd29bb98030b862c06ee56bd5b06b
990dc51251a5294891871d427a90595fd86fbd0d
df7371d70cd17e473fded3938fb3cf922e6f2130
dbfef27b3d5ec5ea19127faf280a7e995a0da72a
eb0d6a426fcbae4c825c513f45440ea3c8d35132
cb0367405622a39bdcfd2f5bb7e7ef326857693b
```

```
# Answer
# https://crackstation.net/

jackazz23
rattin1
014424036
1skarmania
Dancer17
mr.mo609
faltoshi
```

```
koolitx
umkcrn
```

Задание 3

Найдите приватную часть RSA ключа в приложенном репозитории requests.tgz. Подсказка: сперва узнайте формат RSA ключей, а затем вы можете найти ключ руками или с помощью программы https://github.com/dxa4481/truffleHog.

https://stackforgeeks.com/blog/decrypt-with-rsa-privatekey-in-python

```
# Using installation script
curl -sSfL
https://raw.githubusercontent.com/trufflesecurity/trufflehog/main/
scripts/install.sh | sh -s -- -b /usr/local/bin
```

Выводы:

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.
> - https://gb.ru

*Выполнил: ==AndreiM