

Forum:[Hack Forums](#)

Thread: [XOR data with multiple ASCII characters\(secret key\)](#)

The_R - September 7, 2015, 6:41 am

Wel,

My last post was about XORing data with the key no bigger than 255 bytes.
Well the bytearray() is simply explained will change a character like "F" to the ASCII table decimal number "70" Than compares it to the key. So the problem was that the key only can be 255 bytes..
This is easily bruteforceable.

So in my next script the key will be a sentence or a word or whatever that will be compared with the plaintext. This is done to convert every character in the key variable to ASCII number.

Example:

PHP Code

```
<?php
key1 = []
key = "pretty.good.key"
for i in range(len(key)):
    key1.append(ord(key[i]))
the output will be:
PHP Code
<?php
[112, 114, 101, 116, 116, 121, 46, 103, 111, 111, 100, 46, 107, 101, 121]
```

every character in "pretty.good.key" will be converted and compared with the plaintext.

Full script:

PHP Code

```
<?php
import sys
import base64

string = str(raw_input("String to encode with XOR? "))
key1 = []
key = "this.could.be.anything"
for i in range(len(key)):
    key1.append(ord(key[i]))
print key1
bytes = bytearray(string)
for c in range(len(bytes)):
    bytes[c] ^=key1[i]
print "Encrypted: ", bytes

decode = bytearray(bytes)
for v in range(len(decode)):
```

```
    decode[v] ^=key1[i]  
print "Decoded: ", decode
```

The_R - *September 10, 2015, 5:05 am*

I will post this on Pastebin asap when I have 50 posts