

CS535 Network Security Fundamentals

Homework: Symmetric Key Crypto

Gangbaoled Li

19525

Using CTR mode to encrypt and decrypt the message "How are you?"

```
from Crypto.Cipher import AES
from Crypto.Util import Counter
from Crypto import Random
import binascii

key_bytes = 32

def encrypt(key, plaintext):
    assert len(key) == key_bytes

    # Choose a random, 16-byte IV.
    iv = Random.new().read(AES.block_size)

    # Convert the IV to a Python integer.
    iv_int = int(binascii.hexlify(iv), 16)

    # Create a new Counter object with IV = iv_int.
    ctr = Counter.new(AES.block_size * 8, initial_value=iv_int)

    # Create AES-CTR cipher.
    aes = AES.new(key, AES.MODE_CTR, counter=ctr)

    # Encrypt and return IV and ciphertext.
    ciphertext = aes.encrypt(plaintext)
    return (iv, ciphertext)

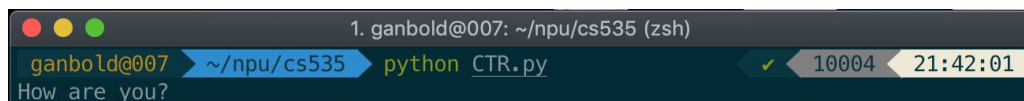
def decrypt(key, iv, ciphertext):
    assert len(key) == key_bytes

    # Initialize counter for decryption. iv should be the same as the output of
    # encrypt().
    iv_int = int(iv.encode('hex'), 16)
    ctr = Counter.new(AES.block_size * 8, initial_value=iv_int)

    # Create AES-CTR cipher.
    aes = AES.new(key, AES.MODE_CTR, counter=ctr)

    # Decrypt and return the plaintext.
    plaintext = aes.decrypt(ciphertext)
    return plaintext

key = '12345678123456781234567812345678'
(iv, ciphertext) = encrypt(key, 'How are you?')
print decrypt(key, iv, ciphertext)
```



A terminal window with a dark background. The title bar shows three colored circles (red, yellow, green) and the text "1. ganbold@007: ~/npu/cs535 (zsh)". The prompt is "ganbold@007" followed by a blue arrow pointing to "~/npu/cs535", then "python" and "CTR.py". The output of the script is "How are you?". On the right side of the terminal, there is a status bar showing a green checkmark, the number "10004", and the time "21:42:01".

Python for RC4

```
#!/usr/bin/python
from Crypto.Cipher import ARC4
from Crypto.Hash import SHA256
from Crypto import Random

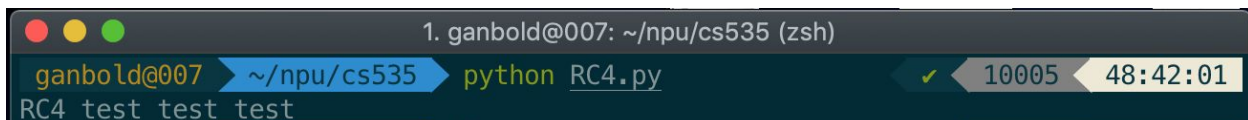
def enc(key, p):
    return ARC4.new(key).encrypt(p)

def dec(key, msg):
    return ARC4.new(key).decrypt(msg)

def main():
    key = 'very long key'
    p = 'RC4 test test test'
    nonce = Random.new().read(16)
    key += nonce
    key = SHA256.new(key).digest() # key is no more than 256bytes

    print dec(key, enc(key, p))

if __name__ == '__main__':
    main()
```



A terminal window with a dark background. The title bar shows three colored circles (red, yellow, green) and the text "1. ganbold@007: ~/npu/cs535 (zsh)". The prompt is "ganbold@007" followed by a blue arrow pointing to the directory "~/npu/cs535". The command "python RC4.py" is entered, followed by a green checkmark icon, the number "10005", and a yellow arrow pointing to the time "48:42:01". The output of the script is "RC4 test test test".

```
1. ganbold@007: ~/npu/cs535 (zsh)
ganbold@007 ➤ ~/npu/cs535 ➤ python RC4.py ✓ 10005 48:42:01
RC4 test test test
```

Discussion board

- A. If you compare the advantages and disadvantages of symmetric key cryptography and asymmetric key cryptography based only on the number of keys each mechanism needs to create. The less the better.

Under what condition, symmetric key cryptography is better?

[Answer] $N < 5$

Under what condition, asymmetric key cryptography is better?

[Answer] $N > 5$

Under what condition, they are tie?

[Answer] $N = 5$ and $N = 0$

What you need to find out are

The range of the number of users when symmetric key cryptography is better than asymmetric key cryptography.

[Answer] (0, 5)

The range of the number of users when symmetric key cryptography is worse than asymmetric key cryptography.

[Answer] (5, infinity)

The range of the number of users when symmetric key cryptography is as good as asymmetric key cryptography .

[Answer] 0 and 5

You can figure out the answers by first figuring out the formulas for
Number_of_keys=f(N)

How many keys are required for N number of users if symmetric key cryptography is used?

[Answer] $f(N) = N * (N - 1) / 2$

How many keys are required for N number of users if asymmetric key cryptography is used?

[Answer] $f(N) = 2 * N$

Comparing the formulas, you will be able to figure out the answers.

B. Why Asymmetric key cryptography alone cannot resolve Internet security issue?

[Answer] Asymmetric key cryptography is slow.

C. Please assess the following statements and give your reasons:

a. Encryption in symmetric key cryptography provides authentication.

[Answer] true

b. Encryption in asymmetric key cryptography provides authentication.

[Answer] false

D. NSA prefers exportable security algorithms easier to break or harder to break?

[Answer] easier to break

E. To achieve the same level of security, which one needs to use a larger key size? Symmetric key cryptography or asymmetric key cryptography? Please explain your assessment.

[Answer] Symmetric key. it's less secure and needs to use large key size.

F. Symmetric key cryptography and asymmetric key cryptography are complimentary. Please explain why and how?

[Answer] To trade off security and speed

G. What are the principal ingredients of a public-key cryptosystem?

[Answer] Plaintext/Ciphertext, Encryption/Decryption, Public and private keys.

H. List and briefly define three uses of a public-key cryptosystem?

[Answer] Confidentiality, Integrity & Authentication.

I. What is the difference between a private key and a secret key?

[Answer] Same

J. How can public-key encryption be used to distribute a secret key?

[Answer] With Hashes