Total points: 75 (+3 bonus)

Assignment 2

Due: 11:59 PM, 9th November

Written assignment

1. Bob runs a social network web server that requires users, such as Alice, to log in. He wants to use cryptography to protect Alice's account. However, he doesn't understand cryptography very well. For each of the below uses of cryptography, identify his mistake, and explain what he should do instead.

   (a) [4 points] Bob obtains a public/private encryption key pair using RSA. When Alice visits his site, Alice generates a 128-bit secret key, encrypts it using Bob's 128-bit public key, and sends it to Bob. Alice and Bob can now use AES (128 bits) to communicate, so they can also use a SHA-256 HMAC to authenticate their messages.

   (b) [4 points] To establish trust, Bob asks a CA to sign his private RSA key using the CA's private ECC key. The CA's public ECC key is in Alice's browser, so Alice can verify Bob's key automatically when she visits his site, even though she does not explicitly know who the CA is.

   (c) [4 points] For Alice's login, Bob requires Alice to hash and salt her password on the client side using SHA-3, and then send it to Bob using 128-bit AES. Then, Bob will store Alice's hashed password and the salt in his database. In future attempts, Alice can use the same hashed password and salt to login.

   (d) [4 points] To store Alice's password securely, Bob uses AES encryption with a secret key and a 64-bit IV to encrypt her password. A CRC32 checksum is used to ensure correctness against random bit flip errors.

2. [9 points] For each of the following network-based attacks in the left column, find the most fitting network defense in the right column. Explain why.

Attack	Defense
IP spoofing	Proxies
Eavesdropping	Deep Packet Inspection
Teardrop attack	Ingress/egress filtering

3. [10 points] When a client C accesses server S through Tor, she usually builds a circuit of three nodes: N_1, N_2, and N_3. A connection is established as follows:

$$C \to N_1 \to N_2 \to N_3 \to S$$

N_1 is also known as the entry node or the guard node, and N_3 is also known as the exit node. Visit `metrics.torproject.org` to answer the following questions:

(a) [3 points] Give the total amount of advertised bandwidth of relays with the "Guard" flag and relays with the "Exit" flag on 2017-01-01. Which is more? Give one reason to explain this phenomenon.

(b) [4 points] Give the median download rate of a file (in bits per second) for a 50 KiB file and a 5 MiB file to the `op-hk` onion server on 2017-06-01. Can you explain the difference?

(c) [3 points] What is a disadvantage of using three nodes in a Tor circuit instead of one node? What is an advantage of doing so?

(d) [3 points (bonus)] Find the list of top 10 countries by number of bridge users. Which, amongst those, is the country with the greatest ratio of bridge users compared to relay users on 2017-06-01? Give the ratio, and suggest why this is the case.

Programming assignment

Cryptography in use [40 points]

(a) [15 points] Two files, `ctext0` and `ctext1`, have been sent to you by e-mail. Those two files were encrypted using the same one-time pad. They are exactly 400 bytes each, and they both come from English Wikipedia articles. Neither file ends with a newline, and all characters are ASCII characters with byte values between 32 and 126. Find the contents of both files using crib-dragging, and submit them as `ptext0` and `ptext1`. (The order does not matter.) You must write your own code to implement crib-dragging; upload all the code you wrote, with file names starting with `cribdrag`.

(b) [5 points] Download Tor and Tor Browser, and browse some of your favorite sites using it. Describe your experience, focusing on at least three ways in which browsing websites with Tor is different from browsing websites normally.

(c) [10 points] Find my PGP public key on the MIT key server, and encrypt a message using GnuPG to that key called `message.asc`. `message.asc` should contain your @connect.ust.hk username (and anything else). Sign it with your own key, and send me the public verification key as `pubring.asc` so I can verify it. Both output files should be **ASCII-armored**. I will test your code using GnuPG with the following command on Ubuntu: `gpg --import pubring.asc` and `gpg message.asc`. My public key fingerprint is:

`0D14 0ABA E8FE C802 6B5F 4DF0 BA82 6122 4AB7 5FBE`

(d) [10 points] Generate a random 128-bit AES key, and put it in `key.txt`. Write any 256-bit message that contains your @connect.ust.hk username, and encrypt it in CBC mode with a chosen IV, and put all of that in `ciphertext.txt` in the following format:

$$IV||Enc_K(M)$$

In the above, || means append, not two copies of the | character. Do not put any extra character between the IV and the ciphertext. Therefore, `key.txt` contains exactly 128 bits (16 bytes), and `ciphertext.txt` contains exactly 128+256 = 384 bits (48 bytes).

You can use someone else's AES implementation here, though you are welcome to implement it.

Submission instructions

All submissions should be done through the CASS system. For this assignment, there is **no** Milestone deadline. Submit the following programs:

- `a2.pdf`, containing all your written answers, including the answers for part (b) of the programming assignment.
- `ptext0` and `ptext1`, for part (a) of the programming assignment, as well as any code necessary to run crib-dragging, in files starting with `cribdrag`. Submit your code; do not submit any compiled files.
- `message.asc` and `pubring.asc`, for part (c) of the programming assignment.
- `key.txt` and `ciphertext.txt`, for part(d) of the programming assignment.

Keep in mind that plagiarism is a serious academic offense; you may discuss the assignment, but write your assignment alone and do not show anyone your answers and code.

The submission system will be closed exactly 48 hours after the due date of the assignment. Submissions after then will not be accepted unless you have requested an extension before the due date of the assignment. You will receive no marks if there is no submission within 48 hours after the due date.