信息安全导论 – Spring 2022

Homework/Lab #1

Due: Monday, March 21th 2022

Highlights

- Expected contribution towards the final score: 6%.
- **You should work on this homework/Lab individually or in a team of up to 3 members (highly recommended). One submission per team.**
- **Submit your work as a pdf** through the USTC Blackboard

1) **(10 points) What are the risks of having the US government select a cryptosystem for widespread commercial use (both inside and outside the United States). How could users from outside the United States overcome some or all of these risks?**

2) **(20 points) Explain why hash collisions occur. That is, why must there always be two different plaintexts that have the same hash value? What property of a hash function means that collisions are not a security problem. That is, why can an attacker not capitalize on collisions and change the underlying plaintext to another form whose value collides with the hash value of the original plaintext?**

3) **(20 points) Identify the CA that has issued the TLS certificate for https://ustc.edu.cn/. Also, identify the certificate expiration date. Besides, export the TLS certificate into a pem file (e.g., through openssl), and calculate its md5 hash and SHA256 hash.**

4) **(30 points) Encrypt/Decrypt/Sign through openssl**
   a) **generation and verificationGenerate an AES-128 key with the cipher mode of CBC through openssl**
   b) **encrypt a message m and decrypt it back using the above AES-128-cbc secrets.**
   c) **Generate a public and private key pair**
   d) **generate a sha256 hash of the message m, and generate a signature by encrypting the hash with your private key**
   e) **Verify the digital signature, with your public key**
   f) **Take screenshots of step a-e, and embed them in the submission pdf.**

5) **(20 points) Read the following paper, summarize its ideas, and give your critical reviews: "New Directions in Cryptography" by Whitfield Diffie and Martin Hellman".**