#1

PB19111701

1

Question:

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?

Answer:

1. The risk comes from the possibility of the existence of government-mandated back-doors in the cryptosystem. That is to say, US government can take advantage of the undetected vulnerabilities of the selected cryptosystem, so that confidential information encrypted by this cryptosystem is transparent to the US government.
2. To overcome this risk, users can encrypt the same message several times by different encryption methods from different cryptosystems. Therefore, vulnerabilities from one of these cryptosystems wouldn't completely ruin the confidentiality of the encrypted message.

2

Question:

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?

Answer:

1. The occurrence of hash collisions is inevitable because the length of $H(m)$ is finite. That is, it is mathematically impossible to map infinite random-length messages to finite hash values of fixed length in one-to-one correspondence.
2. *Collision resistance* (抗碰撞性) is the property keeping hash collisions from being a security problem. In case of *strong collision resistance*, given a hash function H, it is computationally impossible to find two different messages M_1 and M_2, such that $H(M_1) = H(M_2)$. In case of *weak collision resistance*, given a hash function H and a random message M_1, it is computationally impossible to find a message M_2 such that $H(M_1) = H(M_2)$.

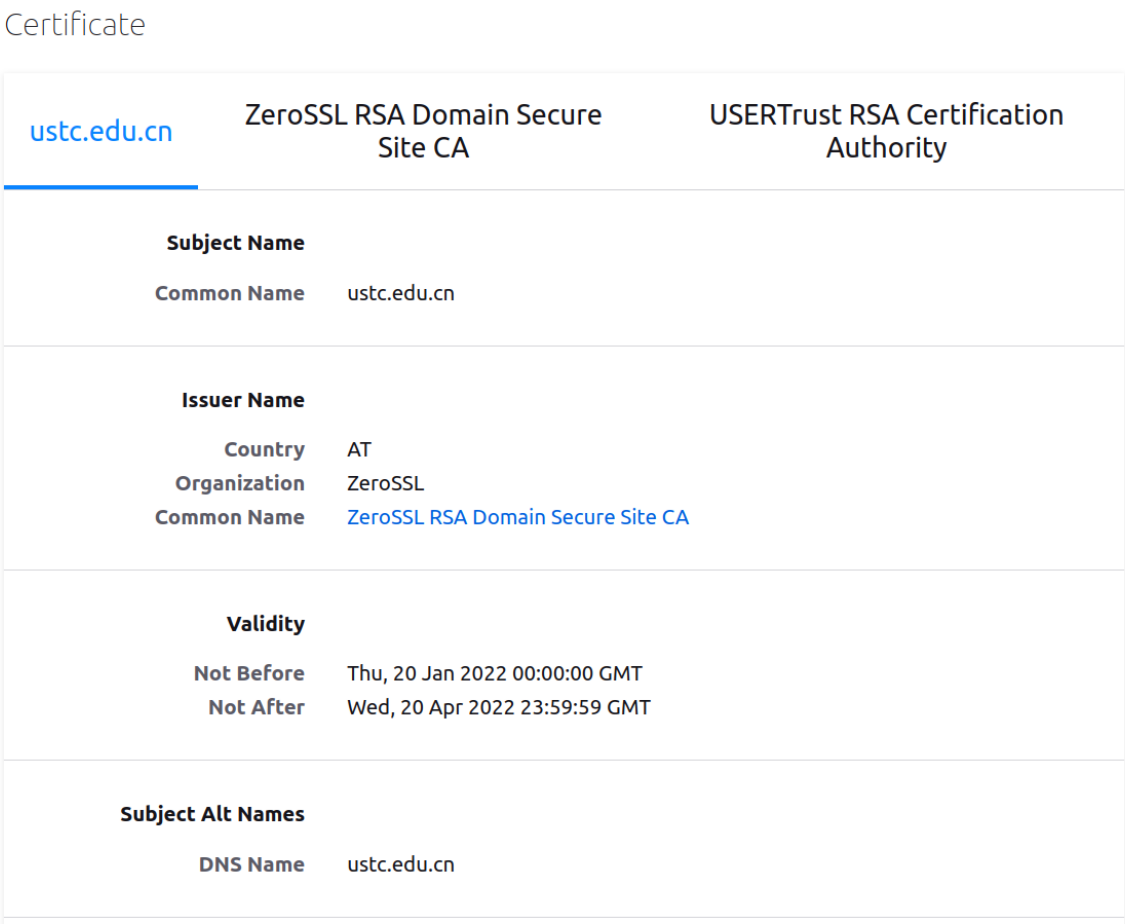
3

Question:

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.

Answer:

Open the website in Firefox and we can get the certificate information as follows:



Therefore, the CA issuing the TLS certificate for the website is **ZeroSSL RSA Domain Secure Site CA**, and the expiration date is **Wed, 20 Apr 2022 23:59:59 GMT**.

Export TLS certificate into a `pem` file, then we can get:

```
(base) ➜ HW1 cat ustc-edu-cn.pem
-----BEGIN CERTIFICATE-----
MIIGZTCCBE2gAwIBAgIRAJ0qTS8dg2Vu5TedxwgMIT8wDQYJKoZIhvcNAQEMBQAw
SzELMAkGA1UEBhMCQVQxEDAOBgNVBAoTB1plcm9TU0wxKjAoBgNVBAMTIVplcm9T
U0wgUlNBIERvbWFpbiBTZWN1cmUgU2l0ZSBDQTAeFw0yMjAxMjAwMDAwMDBaFw0y
MjA0MjAyMzU5NTlaMBYxFDASBgNVBAMTC3VzdGMuZWR1LmNuMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA07xwF4bng4ePRMJJsxyb1LOy6225shuMTKuo
rLjXGP7gwBQG8903+HjdE/q4rYa7CwrNd5tZN4WOLQzfh/wV76/930vUnoOLYFwi
e4C89xwlXOEd9iSy32iISvRIpoX60uTdeyKQNLETdw0P2FGbuQ/k5GPvbzOuRSfl
VGmn/LhDkaEREaD1RPnoiSyy51LJMtRPbiZmWQ1S8ZYYZTXzXVTZh896JNtOuYYs
SqThjnrc51wkwOnMiwx18zX720/nvkgKhh8EZTHeHGnLCA/Ho/BWfvhbuewyMzrD
zb2+p0BQ3vZe94CtfRs+UO4wDoB6DNZpiMwMzKSFzoUhTi9OMQIDAQABo4ICdzCC
AnMwHwYDVR0jBBgwFoAUyNl4aKLZGWjVPXLeXwo+3LWGhqYwHQYDVR0OBBYEFHCD
KGKaNe79xmw38jnJyI751xv/MA4GA1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAA
MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBJBgNVHSAEQjBAMDQGCysG
AQQBsjEBAgJOMCUwIwYIKwYBBQUHAgEWF2h0dHBzOi8vc2VjdGlnby5jb20vQ1BT
MAgGBmeBDAECATCBiAYIKwYBBQUHAQEEfDB6MEsGCCsGAQUFBzAChj9odHRwOi8v
emVyb3NzbC5jcnQuc2VjdGlnby5jb20vWmVyb1NTTFJTQURvbWFpblNlY3VyZVNp
dGVDQS5jcnQwKwYIKwYBBQUHMAGGH2h0dHA6Ly96ZXJvc3NsLm9jc3Auc2VjdGln
by5jb20wggEEBgorBgEEAdZ5AgQCBIH1BIHyAPAAdgBGpVXrdfqRIDC1oolp9PN9
ESxBdL79SbiFq/L8cP5tRwAAAX55hklgAAAEAwBHMEUCIDCQUiZJOBOoFfum8C+1
Nz3IHjpuBDHozVHPw5gJWNxMAiEAhALpQJ3dXoA5GIzBT8Uq5beVCkBjSMg1g56f
FWEcUrAAdgBByMqx3yJGShDGoToJQodeTjGLGwPr60vHaPCQYpYG9gAAAX55hkko
AAAEAwBHMEUCIH+eSL3zCnQrUb1Aq8f8l+wMAgWm5HQsZGecaiUPBaLwAiEAosac
i/p9j5n29TsDaLSLSHpUu3ywjKq697HrdNarYacwFgYDVR0RBA8wDYILdXN0Yy5l
ZHUuY24wDQYJKoZIhvcNAQEMBQADggIBAG5usNF5ymUN7YA3me4K+y3bnMsxEHaB
WWLfFSU8NC5RcHNViTlLzJ23WCPe4GB+LRmnpL7k253R2TX1SoUzsz1mW+YDBuVw
3ELf6l0sAlwCtoyEG2P6b2Vb9Tr5pQmUIYW5O/XljIYSFOWWK6o1gfV6ihl3/eI7
U3mLmnfXsBN32GShFPbRfnBWcEUVmzmZn078IP91l9VnVFIpaRYZb6+firnvR1oG
FDMs0UbYiyPewqdSrfvmBn74o4hT6dQj5Kg1eAkA9ZbgnjPh23ZmcnZ5bsNUHi0Y
L23026xbg/aUaqOO2fnfgNVHLQQGt2xMJrlcUJmJeLcRqNUXF+oqVbQz/x1NwfRB
GOmfLg+VhXavIuRiFQIJCkwYaMh7ZWuLb2yRz4gAzObzpOYJLknwsuheebBDf2aK
byV8HXcWnm3lXWLeiEoye/WWFqe0RNCPKQuLD0OT8yJfhgC0SHfbb+vfC3U6vWHT
l1WdRmsUEE7an1+z1dPNmJQCGAaCNDts45kKv2j++L528cU7NTIIRs+qBtXUxxnV
gKC87+y851QIhjPlg7HEXKCNJUG8EGfBuTNa/VUBHk5cFr/TKqPRQOf5wTXzUZqu
Jn9OOPWnGWHe85Fobe9qu2Y2z5pHSNJj13hxu4fpsUKn8FpU9QGSJ5ka/ucT8qRB
dArEsOsu7Cyi
-----END CERTIFICATE-----
(base) ➜ HW1
```

Calculate its `md5` and `SHA256` hash, the result is showed as below:

```
(base) ➜ HW1 openssl md5 ustc-edu-cn.pem
MD5(ustc-edu-cn.pem)= a2622025c6576e693ac7a3035aa0daf0
(base) ➜ HW1 openssl sha256 ustc-edu-cn.pem
SHA256(ustc-edu-cn.pem)= 5a4138ed2d2b3b2ebbae7dd4243137c2a3b017bf22e7115f3daa0c22b0609400
(base) ➜ HW1
```

4

Question:

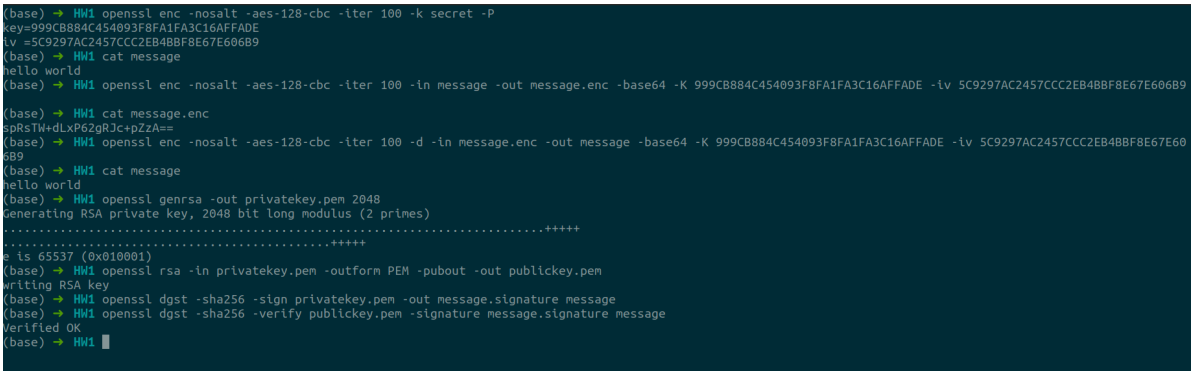
Encrypt/Decrypt/Sign through openssl:

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.

Answer:

> reference: https://wiki.openssl.org/index.php/Command_Line_Utilities



5

Question:

Read the following paper, summarize its ideas, and give your critical reviews: “New Directions in Cryptography” by Whitfield Diffie and Martin Hellman.

Answer:

summary:

1. motivation: minimize the need for secure key distribution channels and supply the equivalent of a written signature;
2. discussions over *public key cryptosystem* and *public key distribution system*;
3. *digital signature* and *one-way authentication* through public key cryptosystem;
4. possibility of extending proofs of security to more useful classes systems with the theory of computaional complexity and analysis of algorithms;

critical reviews:

1. security should be achieved with fewer assumptions (extra conditions) as possible;
2. development of new cryptosystems should meet the comtemporary requests of hardware and software;