Network Security Theory and Practice

1. 10 points: Cryptography

a. What is the difference between symmetric cryptography and asymmetric cryptography?

symmetric cryptography use the same key to encrypt and decrypt, while asymmetric cryptography use different key in decryption and encryption.

b. Given that both types of cryptography can protect security, why should we still need both of them?

The transmission of keys is a problem when using symmetric encryption. People cannot find a secure channel to convey their key. While asymmetric cryptography doesn't need this channel since it doesn't need key transmission.

However, the cost of asymmetric cryptography is large and it's unpractical to apply it into Large-length plaintext encryption. While symmetric cryptography has relative low cost in encryption.

c. What is the algorithm framework of RSA?

Alice generates her RSA keys by selecting two primes: p=11 and q=13. The modulus is n=p×q=143. The totient is n $\phi(n) = (p-1)x(q-1) = 120$. She chooses 7 for her RSA public key e and calculates her RSA private key using the Extended Euclidean algorithm, which gives her 103.

Bob wants to send Alice an encrypted message, M, so he obtains her RSA public key (n, e) which, in this example, is (143, 7). His plaintext message is just the number 9 and is encrypted into ciphertext, C, as follows:

M^e mod n = 9^7 mod 143 = 48 = C

When Alice receives Bob's message, she decrypts it by using her RSA private key (d, n) as follows:

C^d mod n = 48^{103} mod 143 = 9 = M

To use RSA keys to digitally sign a message, Alice would need to create a hash, encrypt the hash value with her RSA private key, and add the key to the message. Bob can then verify that the message has been sent by Alice and has not been altered by decrypting the hash value with her public key. If this value matches the hash of the original message, then only Alice could have sent it -- authentication and non-repudiation -- and the message is exactly as she wrote it -- integrity.

Alice could, of course, encrypt her message with Bob's RSA public key -- confidentiality -- before sending it to Bob. A digital certificate contains information that identifies the certificate's owner and also contains the owner's public key. Certificates are signed by the certificate authority that issues them, and they can simplify the process of obtaining public keys and verifying the owner.

d. What is the key innovation of homomorphic encryption? Provide one use case.

Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The purpose of homomorphic encryption is to allow computation on encrypted data.

In some situations, customers need to use the server (cloud platform) to complete large-scale operations that the client cannot complete, and customers do not want to disclose sensitive data to the cloud platform. At this time, homomorphic encryption is a good technology to apply.

e. How does proxy re-encryption work? What is the design goal?

With the powerful storage capacity of the cloud platform, the data owner encrypts the data with a symmetric key, stores the obtained ciphertext in the cloud, and uses the data owner's public key encryption symmetric key to upload and store the obtained ciphertext to the cloud. . When the data owner Alice wants to share data with Bob, the data owner Alice generates a re-encryption key based on her decryption key and Bob's encryption key, and sends it to the cloud. The cloud server uses its powerful computing power and re-encryption operation in combination with the re-encryption key to store the obtained ciphertext in the cloud. Then Bob downloads two ciphertexts from the cloud server, and decrypts his own private key to obtain the symmetric key, and then decrypts the symmetric key to obtain the original plaintext. In this way, the purpose of ciphertext sharing is achieved, and Alice's private key is not revealed during this entire process.

design goal: There are a lot of data sharing scenarios in the cloud. Because the data owner does not fully trust the cloud service provider, the key to decrypt the ciphertext cannot be sent to the cloud, or the cloud can decrypt and share it. After the data owner downloads the ciphertext and decrypts it, and then encrypts and shares it with the public key of the data receiver, it undoubtedly causes great trouble to the data owner, and also loses the meaning of cloud data sharing. Proxy re-encryption can achieve cloud ciphertext data sharing without revealing the data owner's decryption key.

2. 10 points: Cryptanalysis

a. Given an n-bit password, what is the average trying time for cracking the password using a brute force attack? Provide the detailed derivation.

$$1*\frac{1}{2^n}+2*\frac{2^n-1}{2^n}*\frac{1}{2^n-1}+...+2^n*\frac{1}{2^n}$$

$$=\frac{1+2+3+4+5+...+2^n}{2^n}$$

$$=\frac{(1+2^n)*2^n}{2^n*2}$$

$$=2^{n-1}+\frac{1}{2}$$

b. How to attack a one-time pad encryption?

Key: a secret bit string *s* of length *n*

Message: a bit string m of length *n*

ciphertext: a bit string c of length *n*

- Known-Plaintext Attack;

  for all i=1 to n , $s_i = m_i \oplus c_i$

- Chose-Plaintext Attack;

- Adaptive Chose-Plaintext Attack;
- Chose-Ciphertext Attack;
- Ciphertext-Only Attack.

  xor 2 ciphertext and we actually get the xor of 2 plaintext, then we can crack it by dictionary attack.

c. How does a replay attack work? How to address it?

Replay attack: Replay attack is a network attack against data validity or malicious fraud, repeated network requests. This is usually done by someone intercepting the data and forwarding it, and then resending it.

Defense: Using timestamp or one-time session key.

d. How does a man-in-the-middle attack work? How to address it?

Let's say you received an email that appeared to be from your bank, asking you to log in to your account to confirm your contact information. You click on a link in the email and are taken to what appears to be your bank's website, where you log in and perform the requested task.

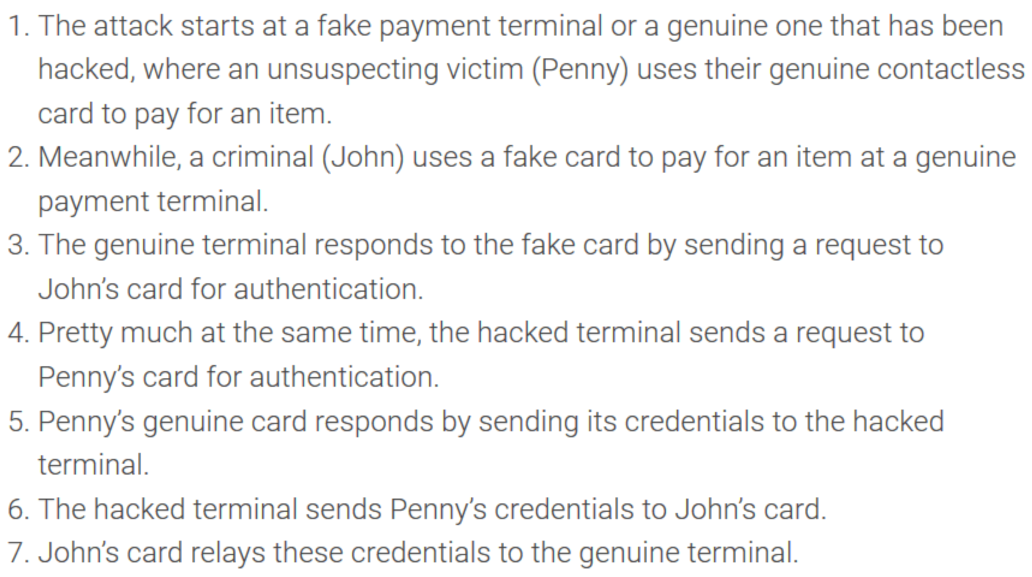
In such a scenario, the man in the middle (MITM) sent you the email, making it appear to be legitimate. (This attack also involves phishing, getting you to click on the email appearing to come from your bank.) He also created a website that looks just like your bank's website, so you wouldn't hesitate to enter your login credentials after clicking the link in the email. But when you do that, you're not logging into your bank account, you're handing over your credentials to the attacker.

MITM Defense

- Make sure "HTTPS" — with the S — is always in the URL bar of the websites you visit.
- **Guarantee Connection Authenticity**, Never connect to public Wi-Fi routers directly, if possible. A VPN encrypts your internet connection on public hotspots to protect the private data you send and receive while using public Wi-Fi, like passwords or credit card information.
- Since MITB attacks primarily use malware for execution, you should install a comprehensive internet security solution, such as Norton Security, on your computer. Always keep the security software up to date.

[]: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

e. How does a relay attack work in wireless communication? How does distance bounding work against a relay attack?



1. The attack starts at a fake payment terminal or a genuine one that has been hacked, where an unsuspecting victim (Penny) uses their genuine contactless card to pay for an item.
2. Meanwhile, a criminal (John) uses a fake card to pay for an item at a genuine payment terminal.
3. The genuine terminal responds to the fake card by sending a request to John's card for authentication.
4. Pretty much at the same time, the hacked terminal sends a request to Penny's card for authentication.
5. Penny's genuine card responds by sending its credentials to the hacked terminal.
6. The hacked terminal sends Penny's credentials to John's card.
7. John's card relays these credentials to the genuine terminal.

The technique of distance bounding could prevent the risk of relay attacks on contactless cards by measuring how long a card takes to respond to a request from a terminal for identification. Since information cannot travel faster than the speed of light, the maximum distance between card and terminal can be calculated. By carefully designing the communication method cards use, this estimate can be made very accurate and ensure that relay attacks over even short distances (around 10m for our prototype) are detected.

Chip & PIN (EMV) relay attacks

3. 10 points: Secure Routing

a. What are the key features of the five typical delivery schemes?

Unicast: deliver a message to a single specific node

Broadcast: deliver a message to all nodes in the network

Multicast: deliver a message to a group of nodes

Anycast: deliver a message to any one out of a group

Geocast: deliver a message to a group of nodes based on geographic location

b. What is the framework of the Dijkstra algorithm?

Let G=(V,E) be a weighted directed graph. Divide the vertex set V into two groups.

The first group is the vertex set whose shortest path has been obtained (represented by S). Start off with just one source point in S. Every time find a shortest path, add it to S. The algorithm ends when all vertices are added to S.

The second group is the set of vertices of the remaining undetermined shortest paths (represented by U). Add the vertices in U to S in the increasing order of the shortest path length. In the process, the shortest path length of each vertex from the source point v to S is always kept to be no greater than the shortest path length of any vertex from the source point v to U. In addition, each vertex corresponds to a distance, the distance of the vertex in S is the shortest path length from v to this vertex. The distance between the vertex in U, from v to this vertex, includes only the current shortest path length of the vertex in S as the intermediate vertex.

Algorithm steps:

- Step 1. Initially, S only contains the source point, that is, S = {v}, and the distance of v is 0. U contains other vertices except v, namely :U={other vertices}. If v and U have edges, then < U,v> normal weight value. If U is not the edge adjacent point of v, then < U,v> weight value is infinity.
- Step 2. Select the vertex k with the smallest distance v from U and add k to S (the selected distance is the shortest path length from v to k).
- Step 3. Take k as the middle point of new consideration and modify the distance of each vertex in U. If the distance from source v to vertex u (through vertex k) is shorter than the original distance (without vertex k), the distance value of vertex u is modified. The distance to the vertex k of the modified distance value plus the edge weight.
- Step 4. Repeat steps 2 and 3 until all vertices are contained in S.

c. What is the framework of the Bellman-Ford algorithm?

Given G(V, E), source point s, array Distant[i] records the path length from source point s to vertex i, initializes array Distant[n], Distant[s] is 0;

For each edge e(u, v), if Distant[u]+c(u, v) < Distant[v], Distant[v] = Distant[u]+c(u, v). c (u,v) is the weight of edge e(u,v); If the operation above does not update the Distant, it means that the shortest path has been found, or that some points are not reachable, out of the loop. Otherwise execute the next loop;

In order to detect whether there is a negative loop in the graph, that is, the loop whose weight sum is less than 0. For each edge e(u, v), if there is an edge and Distant[u] + c(u, v) < Distant[v], there is a negative loop in the diagram, that is, the diagram cannot find a single source shortest path. Otherwise, only the shortest path length from the source point s to each vertex is recorded in the array Distant[n].

d. How does prefix hijacking work?

distance-vector: announce 0 distance to all other nodes

link-state: drop links; claim direct link to any other routers

BGP: announce arbitrary prefix; alter paths

e. How does RPKI work? Why is it insufficient for secure routing?

The RPKI works below:

- Step 1. Verify the code number resource allocation relationship by issuing RPKI resource certificate. When a CA assigns a portion of its IP address resource /AS number to a lower authority, it issues a resource certificate to that authority to confirm the assignment. The content of the certificate is the binding relationship between the IP address prefix /AS number and the receiving institution.
- Step 2. Authorize an autonomous network to issue a routing origin notification to an IP address prefix by issuing a ROA signature. ROA binds the AS number of the autonomous network to the IP prefix.
- Step 3. The above resource certificates and ROA signatures are stored and published in the publish points maintained by each CA, and the distributed database composed of all these publish points is the RPKI database.
- Step 4. The RPKI dependent party (RP) is responsible for periodically downloading these certificates and signatures synchronously from the RPKI database and verifying their validity

to obtain the true authorization relationship between the IP prefix and the AS number. The router obtains this data from the RPKI dependent party to determine the authenticity of the BGP routing message, that is, whether the originating AS in the routing message has the legal authorization to notify the IP prefix.

Insufficient reason: Malicious router can pretend to connect to the valid origin.

4. 10 points: Secure Forwarding

a. What is the difference between routing and forwarding? Why is secure routing insufficient for secure forwarding?

- Routing: select a path for traffic in a network
- Forwarding: relay packets along a certain path

Reason: Because the routing security cannot ensure that the forwarding is carried out according to the route plan, the forwarding security problem exists.

b. In which scenarios should secure forwarding be enforced? If not, what are the security impacts?

In the scenarios of downgrade service quality and bypass attacking-traffic filter, we should enforce the forwarding.

Take the example in the class: some small company buy the service of payload cleaning from some big company to avoid from attacking, but without secure forwarding, the package may bypass the big company's service and the data is insecure.

c. How does a typical secure forwarding scheme, ICING, work?

- PoC: Proof of Consent

  certify the provider’s consent to carry traffic along the path

- PoP: Proof of Provenance

  allow upstream nodes to prove to downstream nodes that they carried the packet

We need to validate that the package is relaying on a certain path and it's following exactly the right orger of nodes.

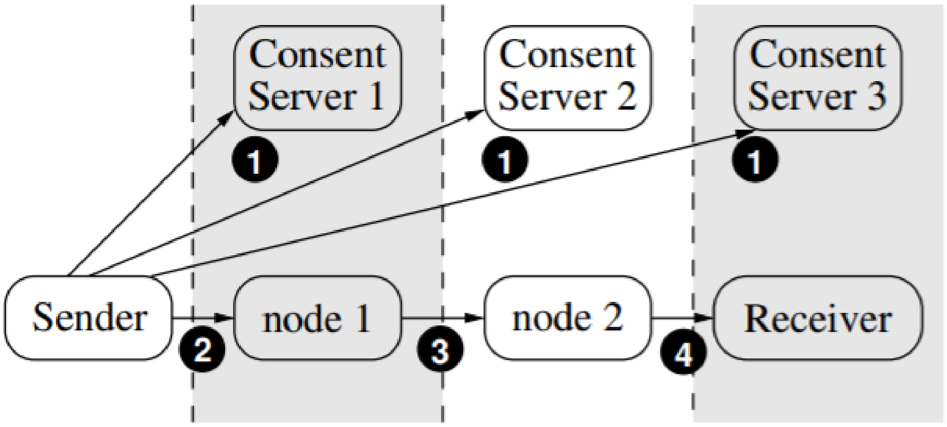


Figure 1—Forwarding in ICING. ❶ The sender logically gets PoCs from the consent servers of all nodes on the path (a consent server can delegate PoC-issuing, making this step lightweight). ❷ The sender creates and sends the packet to the first ICING node, having used the PoCs to construct tokens that ❸ each forwarder verifies and transforms for its successors until ❹ it arrives at the receiver.

5. 10 points: Blockchain

a. What are the key cryptographic techniques used in blockchain? What are they used for therein?

- digital signature:

  The process of opening a bit coin account is the process of creating a pair of public and private keys locally. if A wants to transfer money to B, that is, A initiates a transaction on the blockchain, all transactions are public, but how do you judge that this transaction is indeed initiated by A, not someone else impersonating, this requires A user to use their own Sign the transaction with the private key of. After other users get the signature and transaction information, they can use A's public key to verify the correctness of the signature.

- hash :

  If you want the calculated hash value to fall within a certain range, there is no specific way to construct the input. It is not even possible to know what kind of input is more likely to get a hash value with specific characteristics. If you want to get this kind of input, you can only try one by one, there is no shortcut.

  The process of Bitcoin mining is to find a random number `nonce`. This nonce is combined with other information in the block header as an input, and the hash value is obtained, and the resulting hash value should be less than or equal to a specified threshold.The mining process is to keep trying nonce, so that the hash of the entire block header is less than or equal to the target.

b. How is double spending addressed in blockchain?

When miners pull the transactions simultaneously from the pool, then whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded.

“Confirmations” are nothing but more blocks containing more transactions being added to the blockchain. Each transaction and blocks are mathematically related to the previous one. All these confirmations and transactions are time-stamped on the blockchain, making them irreversible and impossible to tamper with.

It is recommended for merchants to wait for a **minimum of 6 confirmations.** Because to be able to double spend that coin, the sender has to go back and reverse all transactions in the 6 blocks that have been added *after* their transaction, ***which is computationally impossible.***

c. How does Proof of Stake work and save blockchain from intensive computation?

Every participant joins blockchain by paying stake

When choosing creator of a block, more stake with high probability

Creator gets stake reward if created block passes verification, otherwise, penalty

Only one creator per block; no huge computation waste.

6. 10 points: Secure Connection

a. How does a DNS hijacking attack affect network security?

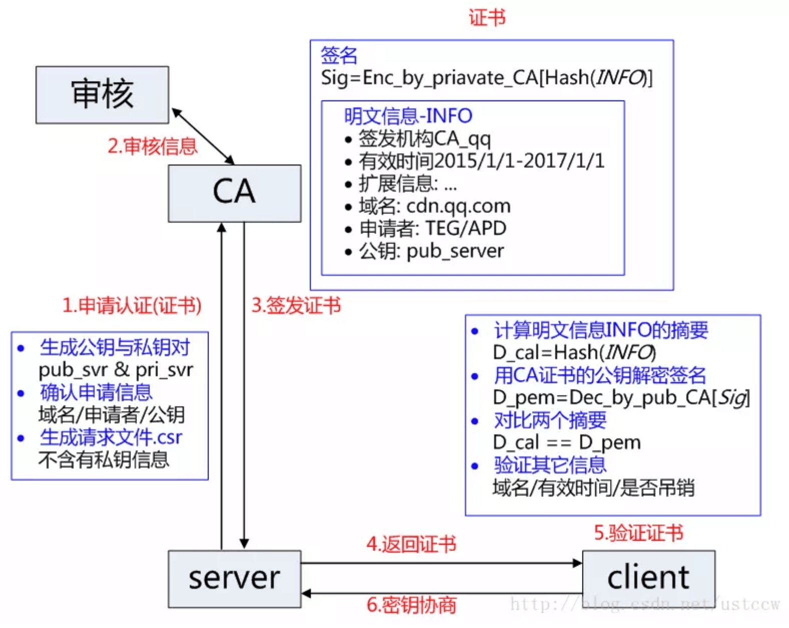
The most common method for DNS Hijacking is to install a malware on your computer that changes the DNS so that whenever your browser tries to resolve a URL, it contacts one of the fake DNS servers instead of real DNS servers that are used by ICANN (authority of Internet that is responsible for registering domains, managing them, providing them with IP addresses, maintaining the contact addresses and more). The direct DNS servers that your computer contacts are the DNS servers being operated by your Internet Service Provider. When an internet connection is bought, the DNS servers in use are of the ISP – recognized by ICANN.

The malware on your computer changes the default DNS trusted by your computer to point to some other IP address. That way, when your browser tries to resolve an IP address, your computer contacts a fake DNS server that gives you wrong IP address. This results in your browser loading a malicious website that may compromise your computer or steal your credentials etc.

b. What is the protocol framework of HTTPS?

1. connection request
2. server response
3. certificate verification
4. key exchange
5. secure communication
6. end

c. How does a user verify a certificate for determining the authenticity of the website it connects to?



1. The certificate must be issued by a trusted Certificate Authority (CA).
2. The fully qualified hostname in the HTTPS request URL and the certificate owner (“Issued to” name) must match.
3. The certificate must be current (within its “Valid from…to…” date range).
4. The certificate must not be on a revocation list (either CRL or OCSP).
5. Checks 1-4 are recursively applied to every certificate in the trust chain.

d. When is a certificate chain required? How to authenticate a certificate chain?

A certificate chain is an ordered list of certificates, containing an SSL Certificate and Certificate Authority (CA) Certificates, that enable the receiver to verify that the sender and all CA's are trustworthy. The chain or path begins with the SSL certificate, and each certificate in the chain is signed by the entity identified by the next certificate in the chain. It's required when we access a website.

Any certificate that sits between the SSL Certificate and the Root Certificate is called a chain or Intermediate Certificate. The Intermediate Certificate is the signer/issuer of the SSL Certificate. The Root CA Certificate is the signer/issuer of the Intermediate Certificate. If the Intermediate Certificate is not installed on the server (where the SSL certificate is installed) it may prevent some browsers, mobile devices, applications, etc. from trusting the SSL certificate. In order to make the SSL certificate compatible with all clients, it is necessary that the Intermediate Certificate be installed.

The chain terminates with a Root CA Certificate. The Root CA Certificate is always signed by the CA itself. The signatures of all certificates in the chain must be verified up to the Root CA Certificate. Root certificate is stored in the client's os.

7. 10 points: Wi-Fi Security

a. What key properties of wireless communication make it more vulnerable to attacks than wired communication?

- Broadcast Communication, which is far more susceptible to eavesdropping and jamming than wired networks.
- Higher Mobility

  far more portable and mobile, thus resulting in a number of risks;

- Constrained Resource

  sophisticated OS but limited memory and processing resources to counter threats, including DoS and malware

- Greater Accessibility

  may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks

b. Why is WEP insecure?

I have applied chop attack to WEP in course *IOT security*, and here is the report. In the report, we simplify the CRC function to a xor operation.

First, we assume the plaintext is [D_1,D_2,D_3,I], key is [K_1,K_2,K_3,K_4], and the cipher is [R_1,R_2,R_3 ,R_4].

the first chop

After the first chop, the plaintext is [D_1,D_2,J_1] and the cipher is [R_1,R_2,S_1].

“If the guess for the chopped byte is correct, the packet will be a valid WEP packet. It will thus be accepted by the access point. If it is invalid, it will be silently discarded.” We can directly get the cipher text S_1 that meets the requirements through brute force search， and S_1 ^ K_3 == J_1.

Then we know： -

$$\begin{gathered} D_1 \oplus D_2 == J_1 \\ D_3 \oplus K_3 == R_3 \\ J_1 \oplus K_3 == S_1 \\ D_1 \oplus D_2 \oplus D_3 == I \end{gathered} \tag{1}$$

Finally, we can get the byte I

$$I == R_3 \oplus S_1 \tag{2}$$

Since S can be brute-forced and cracked, R_3 is a known ciphertext, so the value of I can be calculated directly.

Since $I \oplus R_4$ then we can calculate K_4

the second chop

After the second chop, the plaintext is [D_1,J_1] and the cipher is [R_1,S_1].

Now, J_2 == D_1 , we can find :

$$D_1 \oplus D_2 == S_2 \oplus R_2 \tag{3}$$

Finally,

$$D_3 == I \oplus D_1 \oplus D_2 == R_3 \oplus S_1 \oplus S_2 \oplus R_2 \tag{4}$$

....

Multiple chop attacks can be used to obtain the key.

c. How does IEEE 802.11i provide a higher security guarantee than WEP?

IEEE 802.11i enforces mutual authentication between STA <--> AP.

One of the key elements of the WPA scheme is the use of the TKIP - Temporal Key Integrity Protocol. TKIP is part of the IEEE802.11i standard and operates by performing per-packet key mixing with re-keying.

In addition to this the WPA, Wi-Fi Protected Access scheme also provides optional support for AES-CCMP algorithm. This provides a significantly improved level of security.

The WPA2 scheme for Wi-Fi network security has now superseded the basic WPA or WPAv1 scheme. WPA2 implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.

8. 10 points: Anonymous Communication

a. Why is current Internet communication vulnerable to anonymity or privacy leakage?

For users to communicate via internet, their devices assigned with IP addresses,

which are usually fixed within a communication session or more.

This can be used to infer critical privacy of users.

b. In which scenarios do users require the communication anonymity or privacy as concerned in sub-question a?

- Unmonitored access to health and medical information
- Preservation of democracy:

  anonymous election/jury
- Censorship circumvention:

  anonymous access to otherwise restricted information

c. How to use proxies to secure communication anonymity? What are the possible limitations?

How to use:

- intermediary between sender & receiver
- Sender relays all traffic through proxy
- Encrypt destination and payload
- Asymmetric technique: receiver not involved (or informed of) anonymity

Limitations:

- Require trusted third party proxy, which may release logs, or sell them, or blackmail sender
- Anonymity largely depends on the (likely unknown) location of attacker

d. How does Onion Routing provide a better guarantee for anonymity?

Leverage the overlay network architecture.

- Connect to Tor entry
- Randomly select a series of Tors
- Relay messages across them
- Tor exit relays messages to destination
- Reply traffic from destination traverses the reverse path
- Maintains a bidirectional persistent multi-hop path between source and destination

e. How to infer anonymity or privacy of Onion Routing traffic?

- **Path Selection Attack**

  Tor path selection algorithm: weight nodes by selfreported bandwidth; select each node using weighted probability distribution;

  Attack: malicious relay reports very high bandwidth to increase selection probability;

  if it controls the first hop, de- sender; if it controls the last hop, de- receiver;

- **Counting Attack**

  Correlate incoming and outgoing flows by counting the number of packets

- **Low Latency Attack**

  Tor router assigns each anonymous circuit its own queue

  Dequeue one packet from each queue in round-robin fashion

- **Cross Site Attack**

  Search the accounts on public websites

9. 10 points: Authentication Efficiency

Consider a time-consuming authentication scenario where a database records all secret keys of a large number of users. When the system authenticates a user, it first issues a challenge message to the user. The user then uses his/her key to encrypt the challenge and then returns the encrypted challenge to the system. The system then encrypts the challenge using one key in the database after another and compares the result with the received encrypted message. Once a match is found, the system accepts the user. Otherwise, the user is denied. This authentication protocol surely takes a lot of time and computation.

Design a possible solution to speed up the authentication process.

Client can return its ID with the encrypted message when response.

When the system authenticates a user, it first issues a challenge message to the user. The user then uses his/her key to encrypt the challenge and then returns the encrypted challenge and the user's ID to the system. The system then get the key through the given ID. This method can help reduce calculation time.

666.10 points: SHINE YOUR WAY

Share your thoughts on the course project.

a. Do you aim for a research output from the course project? To what extent do you devote your time and energy to it? How do you overcome the associated challenges?

Yes, but because I'm Inefficient study at home, it seems that I completing the project without too much devotion.

b. Do you think that you have gradually cultivated a research/security mindset? What is the most useful idea that you learned during this process?

Yes, and I think the most useful idea is to exchange ideas with others.

c. Provide an example to showcase how you leverage that useful idea to facilitate problem solving in study or life.

Communication is very important in modern life. And this can help us work efficiently.

Design a question that you think is feasible as an exam question.

a. Which topic among the lectures you would like to consider?

WIFI security, WEP's chop attack

b. Describe a (sufficiently complex) question;

The ChopChop attack unbelievably allows an adversary to decrypt an entire WEP packet without knowing the WEP key. It works by chopping off the last byte of the packet, making a guess for the plain text value of the byte, and then correcting the ICV. The idea is that if the guess for the chopped byte is correct, the packet will be a valid WEP packet. It will thus be accepted by the access point. If it is invalid, it will be silently discarded.

In this problem, the ICV is calculated through XORing all plaintext data in the packets. For instance, in table, ICV = datablock1⊕datablock2⊕datablock3 (**in plaintext**). The ciphertext of each data block is calculated through XORing the plaintext with the key stream.

Assume an adversary has obtained the above ciphertext.

	data block1	**data block2**	**data block3**	**ICV**
original ciphertext	F7	F1	DE	DA
key	a	b	c	d
	data block1	**data block2**	**ICV**	
ciphertext after 1 chop	F7	F1	**4a**	

What's the value of d?

c. Provide also a correct sample solution, thanks.

First, we assume the plaintext is [D_1,D_2,D_3,I], key is [K_1,K_2,K_3,K_4], and the cipher is [R_1,R_2,R_3 ,R_4].

After the first chop, the plaintext is [D_1,D_2,J_1] and the cipher is [R_1,R_2,S_1].

“If the guess for the chopped byte is correct, the packet will be a valid WEP packet. It will thus be accepted by the access point. If it is invalid, it will be silently discarded.” We can directly get the cipher text S_1 that meets the requirements through brute force search， and S_1 ^ K_3 == J_1.

Then we know： -

$$\begin{aligned} D_1 \oplus D_2 &== J_1 \\ D_3 \oplus K_3 &== R_3 \\ J_1 \oplus K_3 &== S_1 \\ D_1 \oplus D_2 \oplus D_3 &== I \end{aligned} \tag{5}$$

Finally, we can get the byte I

$$I == R_3 \oplus S_1 \tag{6}$$

Since S can be brute-forced and cracked, R_3 is a known ciphertext, so the value of I can be calculated directly.

Since $I \oplus R_4$ then we can calculate K_4

$d = R_3 \oplus R_4 \oplus S_1 = 0x4E$