7240389S Chongyu Chang

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY
100 Ping Le Yuan, Chao Yang District, Beijing 100124, China http://www.bjut.edu.cn

Problem 1

In late August 2024, Seattle-Tacoma International Airport (Sea-Tac) faced a major disruption due to a cyberattack that targeted its internet, phone, and email systems. The attack impacted critical airport operations, leading to extended outages that persisted for days. As a result, many travelers experienced significant delays, especially in security screening, check-in, and baggage handling. The baggage sorting system was compromised, causing airlines to advise passengers to avoid checking bags. Terminal information displays were also offline, which led to confusion and required staff to use intercoms to guide travelers.

The attack is believed to have been carried out by an organized cybercriminal group, though specific details about the attackers remain unclear. The main security services compromised included the airport's communication infrastructure, baggage handling systems, and information displays, which are all essential for smooth airport operations. The attackers exploited vulnerabilities that allowed them to disrupt multiple services simultaneously, highlighting the gaps in the airport's cybersecurity measures.

While the TSA's screening operations remained functional, and major airlines like Delta and Alaska Airlines were largely unaffected in their flight schedules, the

outages still led to chaos within the airport. Long security lines, missing luggage, and confusion at gates added to the frustration of passengers. Many travelers found themselves relying heavily on mobile apps for boarding passes, as traditional systems failed.

Port of Seattle officials, with the support of federal agencies like the Transportation Security Administration and Customs and Border Protection, worked to restore the affected systems and investigate the breach. The situation highlighted the vulnerability of large infrastructure to cyber threats and the importance of having contingency plans for maintaining essential airport services during such incidents. Despite their efforts, officials were unable to provide a clear timeline for the restoration of normal operations, leaving both airport staff and travelers in an uncertain state.

To mitigate such events in the future, several services and mechanisms could be employed. Implementing stronger network segmentation could help isolate critical systems, preventing an attack from spreading across the entire network. Enhanced intrusion detection and response systems could also provide early warnings and mitigate the impact of such an attack. Additionally, regular cybersecurity audits and vulnerability assessments could help identify and fix weaknesses before they are exploited by attackers. Backup communication systems and manual contingency processes should also be maintained to ensure continuity of essential services in the event of a cyberattack.

Links:

[1] https://ground.news/article/seattle-tacoma-international-airport-hit-with-delays-after-possible-cyberattack_c0cde0

[2] https://time.news/cyber-attack-shuts-down-internet-at-news-agency-us-seattle-airport/

[3] https://ground.news/article/seattle-tacoma-international-airport-hit-with-delays-after-possible-cyberattack_c0cde0

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY

Problem 2

solve: Method for encryption in CBC, using the shift key is:

$$\begin{cases} Ek(P_0 \oplus IV) = C_1 \\ Ek(P_1 \oplus C_1) = C_2 \\ Ek(P_2 \oplus C_2) = C_3 \text{ and soon} \end{cases} \quad \therefore Ek(P_n \oplus C_n) = C_{n+1}$$

~~$\therefore Ek(P_{n-1} \oplus P_{n-1}) = C$~~

(a) $C_1 = Ek(P_0 \oplus IV) = Ek(C(0010) = F$

$C_2 = Ek(P_1 \oplus C_1) = Ek(L(1011)) = 0$

$C_3 = Ek(P_2 \oplus C_2) = Ek(P(1111)) = C$

$$\therefore \begin{cases} C_4 = Ek(P_3 \oplus C_3) = F \\ C_5 = Ek(P_4 \oplus C_4) = B \\ C_6 = Ek(P_5 \oplus C_5) = M \\ C_7 = Ek(P_6 \oplus C_6) = B \\ C_8 = Ek(P_7 \oplus C_7) = I \end{cases}$$

∴ Its ciphertext is FOCFBMBI.

(b) As the same way:

we have: $C_1 = Ek(P_0 \oplus IV) = O$ $\quad C_5 = Ek(P_4 \oplus C_4) = G$

$C_2 = Ek(P_1 \oplus C_1) = D$ $\quad C_6 = Ek(P_5 \oplus C_5) = B$

$C_3 = Ek(P_2 \oplus C_2) = F$ $\quad C_7 = Ek(P_6 \oplus C_6) = G$

$C_4 = Ek(P_3 \oplus C_3) = I$ $\quad C_8 = Ek(P_7 \oplus C_7) = F$

∴ Its ~~chiper~~ cipher text is ODFIGBGF.

[In fact, the ~~series~~ number of subscript is 0~7 is better.]

(c) This time, we have:

$C_0 = P_0 \oplus E_K(IV) = 0001 \oplus 0011 = 0010 = C$

$\therefore C_1 = P_1 \oplus E_K(IV+1) = 1110 \oplus 0100 = 1010 = K$

$C_2 = P_2 \oplus E_K(IV+2) = E$

$C_3 = P_3 \oplus E_K(IV+3) = G$

$C_4 = P_4 \oplus E_K(IV+4) = M$ ∴ the C = (CKEGMALO)

$C_5 = P_5 \oplus E_K(IV+5) = A$

$C_6 = P_6 \oplus E_K(IV+6) = L$

$C_7 = P_7 \oplus E_K(IV+7) = O$

~~$C_8 = P_8 \oplus E_K(IV+8) = \oplus$~~

(d) This time, $C_3' = 1010$ (MSB of $C_3 = 0010$ is 0010).

$P_0' = D_K(C_0) \oplus IV$

$= E_K^{-1}(C_0) \oplus IV$

$= 0011 \oplus 0010 = 0001 = B$

At the same time, $P_1' = D_K(C_1) \oplus C_0 = E_K^{-1}(C_1) \oplus C_0 = O$

$P_2' = D_K(C_2) \oplus C_1 = E_K^{-1}(C_2) \oplus C_1 = B$

do not be affected.

From P_3', we have ~~$P_3' = D_K(C_3) \oplus$~~ changes which begin at:

$P_3' = D_K(C_3') \oplus C_2 = E_K^{-1}(C_3') \oplus C_2 = I$ [A]

$P_4' = D_K(C_4) \oplus C_3' = E_K^{-1}(C_4) \oplus C_3' = D$ [I]

$P_5' = D_K(C_5) \oplus C_4 = E_K^{-1}(G) \oplus C_4 = I$

$P_6' = D_K(C_6) \oplus C_5 = E_K^{-1}(C_6) \oplus C_5 = C$

$P_7' = D_K(C_7) \oplus C_6 = E_K^{-1}(C_7) \oplus C_6$ E

∴ the recovered type is (BOBI DICE)

(e) This time ∴ From ~~the~~ P_0'' to P_{12}', No change.

$C_0'' = C_0 = 0101$ ∴ $P_0'' = B$ $E_K^{-1} D_K(C_{00}'') \oplus IV = B$

$C_1'' = C_1 = 1110$ $P_1'' = 0$ $D_K(C_1'') \oplus C_0'' = 0$

$C_2'' = C_2 = 0010$ $P_2'' = B$ $D_K(C_2'') \oplus C_1'' = B$

~~From the~~ b The change begins at C_{30}''

$C_3'' = C_4 = 0001$, $C_4'' = C_5 = 1100$, $C_{50}'' = C_6 = 0001$, $C_6'' = C_7 = 1000$

∴
$P_{30}'' = C_2'' \oplus D_K(C_3'') = C_2'' \oplus E_K^{-1}(C_3'') = 1100 = M$

$P_4'' = C_{30}'' \oplus D_K(C_4'') = I$

$P_5'' = C_4'' \oplus D_K(C_{50}'') = C$

$P_6'' = C_5'' \oplus D_K(C_{60}'') = E$

∴ The recovered text is (BoBMICE).

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY

Problem 3

solve: From the text of the problem, we have:

$$\begin{cases} X = 7240\,3895 \\ Y = 3895 \end{cases}$$

$\therefore 41^{3895} \mod 18865$

$= 41^{2048+1024+512+256+32+16+4+2+1} \mod 18865$

~~$= 41^{(0111)_2} \mod 18865$~~

$= 41^{16+10+9+8+5+4+3+2+1} \mod 18865$

@ We use calculator, the result is

~~$= (41 \times 168 \times 8926 \times 79$~~

$= (41 \times 168 \times 14876 \times 8926 \times 6581 \times 16626 \times 13896 \times 1554 \times 1295) \mod 18865$

$= (12326 \times 11306 \times 7571 \times 10081 \times 1295) \mod 18865$

$= 13\,55$

(b)

~~$\phi(Y)$~~ ∵ $3895 = 41 \times 19 \times 5$

$\therefore \phi(Y) = (41-1)(19-1)(5-1) = 2880$

(c) $\gcd(7240\,3895, 928374827)$

∴ We can use Euclidean algorithm to find GCD, we found they are co-prime.

$\therefore \gcd(7240\,3895, 928374827) = 1$

(d) ∵ they are Coprime.
∴ According to the extend Euclidean algorithm
we trace back the ~~mo~~ process of (c)

$$\text{we can have } \begin{cases} x = -26731871 \\ z = 20833598 \end{cases}$$

(e) ∵ $\gcd(29145_2, 08809) = 1$
∴ When we trace back:

~~$29145_2 = 2 \times 08809 + 73834$~~

$1 = 3 - 1 \times 2$
$= 3 - 1 \times (8 - 2 \times 3)$
$= -1 \times 8 + 3 \times 3$
$= -1 \times 8 + 3 \times (19 - 2 \times 8) = 3 \times 19 - 7 \times 8$
$= 3 \times 19 - 7 \times (3884 - 204 \times 19) = -7 \times 3884 + 1431 \times 19$
$= -7 \times 3884 + 1431 \times (34975 - 9 \times 3884) = 1431 \times 34975 - 12886 \times 3884$
$= 1431 \times 34975 - 12886 \times (73834 - 2 \times 34975) = -12886 \times 73834 + 27203 \times 34975$
$= -12886 \times 73834 + 27203 \times (108809 - 1 \times 73834) = 27203 \times 108809 - 40089 \times 73834$
$= 27203 \times 108809 - 40089 \times (291452 - 2 \times 108809) = -40089 \times 291452 + 107381 \times 108809$

∴ $1 \bmod 291452$
$= -40089 \times 291452 + 107381 \times 108809 \bmod 291452$
$= 107381 \times 108809$
∴ 107381 is $108809^{-1} \bmod 291452$

(f) We'd like to choose ~~X~~ z=2

Since $X = 7240\,3895 = [7240\,3894 + 1]$

$\therefore \quad x^x \bmod 2$

$= [7240\,3895]^{7240\,3895} \bmod 2$

$= [7240\,3894+1]^{7240\,3895} \bmod 2$

According to the Binomial Theorem.

we have:

$x^x \bmod 2 = C_{7240\,3895}^{0} \cdot (1)^{7240\,3895} \bmod 2$

$= 1 \bmod 2 = 1$

Problem 4

Solve: (a)

When $P=13$ & $g=3$,

private key is $x=5$

$\therefore y = g^x \bmod P = 3^5 \bmod 13 = 243 \bmod 13 = 9$

(b) sender got $(P,g,y)=(13,3,9)$

He set $r=7$

$\therefore$ He had ~~$M=6$~~ $M=6$

$\therefore \begin{cases} C_1 = g^r \bmod p = 3^7 \bmod 13 = 6561 \bmod 13 = 3 \\ C_2 = (My^r) \bmod p = 6 \cdot 9^7 \bmod 13 = 6 \cdot 3^7 \cdot 3^7 \bmod 13 = 2 \end{cases}$

$\therefore C = C(C_1, C_2) = (3,2)$

(c) $\begin{cases} K = C_1^x \bmod p = 3^5 \bmod 13 = (9 \times 1) \bmod 13 = 9 \\ M = C_2 K^{-1} \bmod p = 2 \cdot 9^{11} \bmod 13 = 6 \end{cases}$

Problem 4 (d)

According to Lecture01.pptx P28.

The El-Gamal encryption algorithm provides the following security services:

(1)Confidentiality

El-Gamal ensures the confidentiality of messages by encrypting them with the recipient's public key, which ensures that only the intended recipient, with the corresponding private key, can decrypt the message. This prevents unauthorized third parties from accessing sensitive information.

(2)Integrity

Similar to authentication, El-Gamal itself does not provide integrity protection, but this can be ensured through the use of digital signatures. By signing the message, the sender ensures that the message has not been altered in transit.

(3)Authentication

While basic El-Gamal encryption does not inherently provide authentication, it can be combined with digital signatures to achieve this. The sender can sign the message or its hash with their private key, and the recipient can verify the signature using the sender's public key, ensuring the message's origin is trustworthy.

(4)Non-repudiation

With digital signatures, the El-Gamal encryption system can provide non-repudiation.

The signature ensures that the sender cannot deny having sent the message, as only the sender possesses the corresponding private key to generate the signature.

(Besides, according to Lecture4.pptx)

(5)Digital Signatures

El-Gamal can be used to create digital signatures. The sender can sign a message with their private key, and the recipient can verify the signature with the sender's public key. This ensures the integrity of the message and the identity of the sender.

(6)Key Exchange

El-Gamal can be employed for key exchange protocols, allowing two communicating parties to negotiate a shared secret key over an insecure channel, which can then be used for subsequent symmetric encryption communication.

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY

Problem #5

① solve:

(a) key from Alice, we can plug P=13, g=7, X=5 in

To get $g^X \bmod p$

$\therefore$ key $= 7^5 \bmod 13$

$= (49 \cdot 49 \cdot 7) \bmod 13$

$= 10 \cdot 10 \cdot 7 \bmod 13$

$= 700 \bmod 13$

$= 11$

(b) key from Bob, we can plug y=11, p=13, g=7 in

To get $g^y \bmod p$

$\therefore$ key $= 7^{11} \bmod 13$

$= 7^5 \cdot 7^5 \cdot 7 \bmod 13$

$= 11 \cdot 11 \cdot 7 \bmod 13$

$= 847 \bmod 13$

$= 2$

(c) $K = g^{xy} \bmod p$

$= 7^{5 \times 11} \bmod 13$

$= 7^{55} \bmod 13$

$= 11^{11} \bmod 13$

$= 6$

Let's check what Bob gets: $K' = 2^5 \bmod 13 = 6 = 6$

$\therefore K = 6$ is acceptable and correct.

Problem 5 (d)

(1)Digital Signatures: Incorporating digital signatures during the DH key exchange is a common solution. Digital signatures verify the authenticity of public keys and ensure that the messages exchanged during the key exchange have not been tampered with. Specifically, parties exchange digital signatures along with their public keys. This way, any third party cannot spoof a public key because only the true public key can produce a valid signature.

(2)Authenticated DH Protocols: Protocols such as Station-to-Station (STS) or Internet Key Exchange (IKE) combine DH key exchange with digital signatures to provide authentication.

(3)Using TLS: When using DH algorithms in the TLS handshake, certificates and digital signatures are combined to prevent MITM attacks.

(4)Ephemeral DH (DHE): In TLS, using temporary DH parameters (i.e., DHE) provides forward secrecy, ensuring that even if long-term keys are compromised, past sessions remain secure.

(5)Key Derivation Functions (KDFs): Functions like HKDF are used to mix the DH generated shared secret with other information (such as message digests) to produce the final session key.

(6)Cryptographic Hash Functions: Including cryptographic hash functions in the DH exchange messages ensures the integrity and authenticity of the messages.

(7)Hardware Security Modules (HSMs): HSMs can securely generate, store, and use keys, reducing the risk of MITM attacks.

(8)Network Layer Encryption: Using IPsec or other VPN technologies to encrypt data at the network layer means that even if the key exchange is tampered with, the attacker cannot decrypt the transmitted data.

Assumptions:

- The communicating parties possess public key certificates issued by a trusted certificate authority.
- The communication environment is at risk of MITM attacks.
- Additional cryptographic algorithms or materials are required, such as digital signature algorithms, key derivation functions, and hash functions.

Notation of Problem 3'

g : The base generator in DH protocol.

P : A large prime number defining the group of the DH protocol.

A & B : Parties involved in the DH key exchange.

k_A & k_B : Private keys of the parties.

y_A & y_B : Public keys of the parties.

K : The shared secret derived from the DH key exchange.

H : A cryptographic hash function

Sign : The digital signature function

Verify : The function to verify digital signatures

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY
100 Ping Le Yuan, Chao Yang District, Beijing 100124, China http://www.bjut.edu.cn

Problem 6

HMAC = h(k||data) is obviously wrong.

Actually HMAC = h(opad ⊕key || h(ipad ⊕key||data))

e.g. i.e. Ipad = 0x3636...

Opad = 0x5c5c...

Here's why the proposed implementation is insecure:

(1)Direct Exposure of Key Material: By concatenating the key directly with the data, the key material is exposed and can be easily extracted from the HMAC value. This defeats the purpose of using a key, as an attacker could potentially use the exposed key to forge HMACs.

(2)Lack of Key Processing: In a proper HMAC implementation, the key is processed to ensure that it is the correct length for the hash function being used. If the key is too long, it is hashed; if it is too short, it is padded.

(3)Vulnerability to Attacks: The proposed method does not provide the necessary security against attacks such as length extension attacks, where an attacker could potentially append data to the original message without knowing the key. Here is the correct way to implement an HMAC, as defined by RFC 2104:

(1)Key Preparation: If the key is longer than the block size of the hash function, hash it to shorten it. If the key is shorter than the block size, pad it to the correct length.

(2)Processing: XOR the prepared key with the inner padding (ipad), which is usually a string of bytes where each byte is 0x36. Append the data data to the result of the XOR operation. Hash the combined value.

(3)Final HMAC Calculation: XOR the prepared key with the outer padding (opad), which is a string of bytes where each byte is 0x5C. Take the hash result from the first step. Append the hash result to the XORed key with opad. Hash the final combined value.

(4)Output: The output of the last hash function is the HMAC.