QUEEN'S UNIVERSITY FINAL EXAMINATION
FACULTY OF ENGINEERING AND APPLIED SCIENCE
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

ELEC 473 – Dr. Jianbing Ni
December 19, 2020

INSTRUCTIONS TO STUDENTS:
This examination is 3 HOURS in length.
There are two sections to this examination.
Please complete an Academic Integrity Statement before gaining access to this exam.
Please answer all questions and upload a PDF file with digital files or images of answers in OnQ.

The final exam is 'closed book', and you are proctored by Proctortrack; the final exam must be completed independently, and you are not permitted to work in groups or to get assistance from any other person. You must answer the final exam entirely on your own. You are not permitted to use social media, texting, online chatting, or email to share questions/answers or to collaborate with anyone during the final exam. Sharing your questions/answers on any platform is not permitted. Any departures from the principles of academic integrity will be investigated and there will be consequences for anyone who is found to have violated these principles. To be clear, anyone who is found to have failed to adhere to the principles of academic integrity on the final exam will automatically get assigned a grade of zero on the final exam and will fail the course.

Put your name and student number on all pages of all answer booklets.
GOOD LUCK!

PLEASE NOTE:
The course instructional team will not be answering questions about the remote exam, aside from possible technical issues or procedural problems. Do your best to answer exam questions as written. If you run into technical issues during the exams, please contact the instructor or the ITSC Exam Support Chat through LiveChat at https://examchat.queensu.ca or call 613-533-6666

Part I Multiple Choices - please mark the best answer (subtotal: 30 marks).

1. DES was selected as an official Federal Information Processing Standard (FIPS) for the United States in

A. 1975

B. 1976

C. 1977

D. 1978

2. Which one of the following algorithms does not belong to asymmetric-key cryptography?

A. RSA algorithm

B. Diffie-Hellman Key Agreement algorithm

C. Message Authentication Code algorithm

D. None of the mentioned

3. RSA stands for:

A. Rivest, Shamir and Adleman

B. Rock, Shane and Amozen

C. Rivest, Shane and Amozen

D. Rock, Shamir and Adleman

4. The elliptic curve group is defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is P + Q, if P = (0, -4) and Q = (1, 0)?

A. (15, -56)

B. (-23, -43)

C. (69, 26)

D. (12, -86)

5. Which statement is FALSE?

A. The key length of 128 bits is sufficient for long term (several decades) security even if practical quantum computers are present.

B. Obtaining a secret key by measuring the electrical power consumption of a processor which operates on the secret key is an example of side-channel analysis.

C. Kerckhoff's Principle means that a cryptosystem should be secure even if an attacker knows all details about the system, with the exception of the secret key.

D. All encryption schemes from ancient times until 1976 were symmetric ones.

6. What is the block cipher structure in DES?
A. Substitution-Permutation Network
B. Feistel Network
C. Rijndael
D. One-way Permutation

7. Which one of the following statements about IPsec protocol is correct?
A. AH supports authentication and integrity. ESP supports confidentiality, authentication, and integrity.
B. AH supports authentication, integrity and confidentiality. ESP supports confidentiality and integrity.
C. AH supports authentication and confidentiality. ESP supports integrity and authentication.
D. AH supports authentication, integrity and confidentiality. ESP supports confidentiality and authentication.

8. In SHA-3, for a message digest size of 256, what is the rate 'r' if the security capacity is 512?
A. 576
B. 832
C. 1088
D. 1152

9. Cryptographic hash function takes an arbitrary block of data and returns
A. fixed size bit string
B. variable size bit string
C. both fixed size bit string and variable size bit string
D. none of the mentioned

10. Which of the following is not a block cipher operating mode?
A. ECB
B. CBF
C. OFB
D. CBC

11. H: $X^{\leq L} \rightarrow T$ is a C.R. Merkle-Damgard Hash Function, a MAC is constructed as MAC(k,m)= H(k ll m). This MAC is insecure because: (PB is the padding block)
A. Given H(k ll m) can compute H(w ll k ll m ll PB) for any w.
B. Given H(k ll m) can compute H(k ll m ll w) for any w.
C. Given H(k ll m) can compute H(k ll m ll PB ll w) for any w.
D. Anyone can compute H(k ll m) for any m.

12. Which permutation is most important for the security measures in DES?
A. Expansion function
B. P-Permutation
C. Permuted Choice-1 and Permuted Choice-2
D. S-boxes

13. How many bit-output is generated by SHA-1?
A. 128
B. 160
C. 256
D. 512

14. Which of the following is an advantage of public-key cryptography over symmetric-key cryptography?
A. Public-key cryptography provides more security services
B. Public-key cryptography does not rely on conjectured hardness of certain computational problems
C. Public-key cryptography has higher throughput
D. Public-key cryptography has shorter key size

15. Which of the following cryptographic algorithms should be used for ensuring integrity and authenticity of a message?
A. SHA1
B. RSA encryption
C. SHA1-based HMAC
D. AES-based ECB mode

16. Consider the following system of two equations (congruences):

$$x \equiv 12 \bmod 29$$
$$x \equiv 7 \bmod 15$$

According to Chinese Remainder Theorem (CRT), which of the following is true about x?
A. x has no solution in (mod $29 \cdot 15$)
B. x has exactly one solution in (mod $29 \cdot 15$)
C. x has more than one solution in (mod $29 \cdot 15$)
D. x has four solutions in (mod $29 \cdot 15$) because there are two equations

17. Suppose a prime $p \equiv 3 \bmod 4$ and $a \in Z_p$. Which of the following is equivalent to a square root of a mod p?
A. $a^{p-1} \bmod p$
B. $a^{(p+1)/4} \bmod p$
C. $a^{(p+1)/2} \bmod p$
D. $a^{(p-1)/2} \bmod p$

18. Which is the weakness in public-key infrastructure (PKI)?
A. Key escrow
B. Non-repudiation
C. Complex certificate management
D. Identity revocation

19. Which one of the following statements about hash function is incorrect?
A. If a hash function is strong collusion resistant, it must be second pre-image resistant.
B. If an adversary can solve the preimage problem of the hash function, he must be able to find a collusion.
C. If a hash function is weak collusion resistant, it must be second pre-image resistant.
D. If an adversary can find a collusion of the hash function, he must be able to solve the second pre-image problem.

20. Which protocol provides either authentication or encryption, or both, for packet at IP level?
A. AH
B. ESP
C. SSL/TLS
D. Kerberos

21. In tunnel mode, IPsec protects the _____
A. Entire IP packet
B. IP header
C. IP payload
D. IP trailer

22. Which two types of IPsec can be used to secure communications between two LANs?
A. AH tunnel mode and AH transport mode
B. ESP tunnel mode and ESP transport mode
C. AH tunnel mode and ESP tunnel mode
D. ESP transport mode and AH transport mode

23. Which one of the following statements about the TLS protocol is incorrect?
A. The alert protocol is used to convey TLS-related alerts to the peer entity.
B. The handshake protocol is done before any application data is transmitted.
C. After the change cipher spec message, both the client and server use the newly negotiated cipher spec and keys to securely exchange the application data.
D. The record protocol serves to build TLS session using the session state parameters.

24. TLS handshake protocol refers to
A. confirming that one of the many lines of communication between the sending client and receiving server is not already in use.
B. sending an electronic key attached to the message so that the receiving server can be unlocked as the message is coming in.
C. verifying that the message sender and message receiver have available communication channels that intersect in the middle.
D. establishing a secure communications path between the message sender and receiver.

25. Which one of the following protocols is designed to provide security and compression services to data generated from the application layer.
A. IPsec
B. SSL/ TLS
C. Kerberos
D. VPN

26. IKE creates security association (SA) for
A. TLS
B. IPsec
C. Kerberos
D. Radius

27. Which one of the following statements about EAP is incorrect?
A. EAP typically rides on top of another protocol such as 802.1x, PPP, or RADIUS.
B. EAP over LAN defines the encapsulation of the EAP over IEEE 802.
C. EAP is a specific authentication mechanism independent to link layer.
D. EAP provides a generic transport service for the exchange of authentication information between a client and an authentication server.

28. Which three functional areas are provided by IPsec?
A. Authentication, Confidentiality, and Key management
B. Authentication, Confidentiality, and Digital Signatures
C. Authentication, Key generation, and Certificate exchange
D. Encryption, Decryption, and Certificate validation

29. How many rounds has DES?
A. 10
B. 12
C. 14
D. 16

30. Let C(K, M) denote a message authentication code function, produced for the message M and a shared key K. Let E(K, M) denote encryption of a message M with a key K, and let || denote the concatenation. If Alice sends to Bob the following information: $E(K_2, M) \,||\, C(K_1, E(K_2, M))$ where K_1 and K_2 are shared secret keys, it is
A. just a message authentication
B. message authentication and confidentiality where authentication is tied to the plaintext
C. message authentication and confidentiality where authentication is tied to the ciphertext
D. message authentication and confidentiality where authentication is tied both to the plaintext and to the ciphertext

Part II (subtotal: 70 marks).

Q1. (14 marks) Please answer the following questions about key establishment.

a. What is the difference between a key agreement protocol and a key distribution protocol?

b. Describe the Diffie-Hellman key agreement protocol.

c. Describe the man-in-the-middle attack against Diffie-Hellman key agreement protocol.

d. Describe the improvement on the Diffie-Hellman key agreement protocol to resist the man-in-the-middle attack.

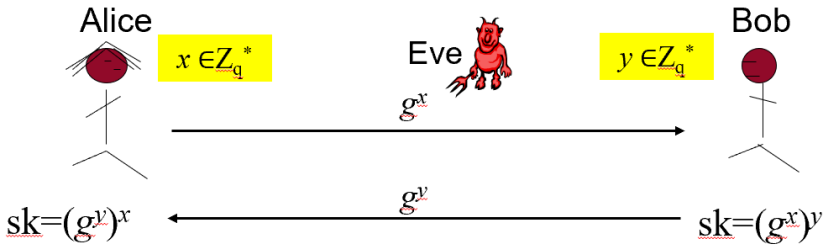
e. Describe the clogging attack against Diffie-Hellman key agreement protocol

a. Key distribution protocol: A key distribution center (KDC)/TA chooses session keys and distributes them to users via an interactive session key distribution scheme.

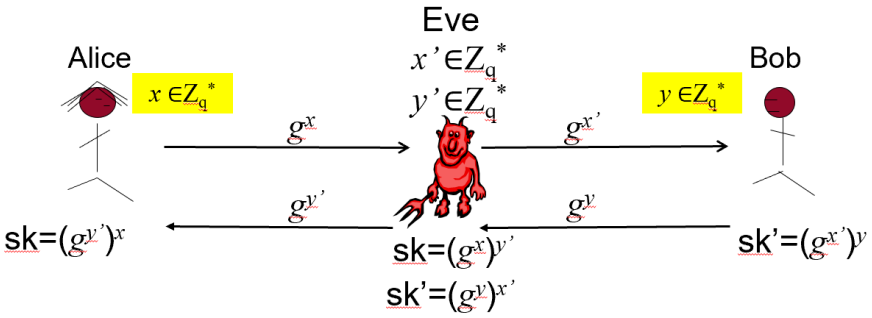
Key agreement protocol: Users employ an interactive key agreement scheme to negotiate a session key over a public channel.

p is a large prime, $q|\ p\text{-}1$, g has the order q in Z_p^*.

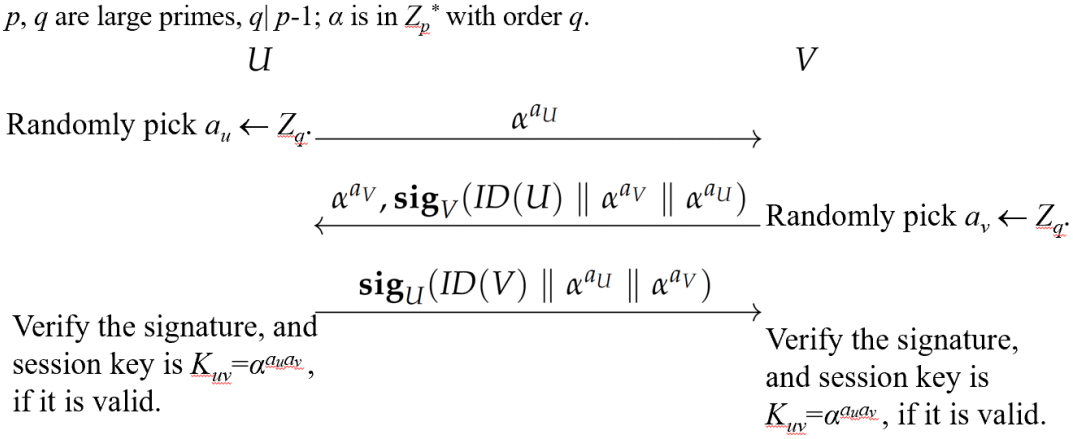
b.



c.



d.



e. Clogging attack: an attacker forges the source address of a legitimate user and sends a public Diffie–Hellman key to the victim. The victim then performs a modular exponentiation to compute the secret key. Repeated messages of this type can *clog* the victim's system with useless work..

Q2. (12 marks) The Kerberos protocol allows a client and an application server to authenticate each other over an insecure network. Please describe the detailed process of the Kerberos protocol that provides this function.

(1) **C → AS** $ID_c \| ID_{tgs} \| TS_1$

(2) **AS → C** $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(3) **C → TGS** $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) **TGS → C** $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(5) **C → V** $Ticket_v \| Authenticator_c$

(6) **V → C** $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

Q3. (12 marks) For n=pq, where p and q are distinct odd primes, define

$$\lambda(n)=\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}.$$

Suppose that we modify the RSA cryptosystem by requiring that ed≡1 mod λ(n).
a. Prove that encryption and decryption are still inverse operations in this modified cryptosystem.
b. If p=41, q=37, and e=7, compute d in this modified cryptosystem.

a. $ed \equiv 1 \bmod \lambda(n) \Rightarrow ed = k\lambda(n)+1, k\in\mathbb{Z}$

If $\gcd(m,n)=1 \Rightarrow \gcd(m,p)=1$, $m^{\lambda(n)} \equiv m^{\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}} \equiv m^{(p-1)\frac{q-1}{\gcd(p-1,q-1)}} \equiv 1 \bmod p$

$\gcd(m,q)=1$, $m^{\lambda(n)} \equiv m^{\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}} \equiv m^{(q-1)\frac{p-1}{\gcd(p-1,q-1)}} \equiv 1 \bmod q$.

If $\gcd(m,n)\neq 1 \Rightarrow$ ~~$\gcd(m,p)>1$~~

$m=xp$ or $m=yq$. $x\in\mathbb{Z}_q^*$. $y\in\mathbb{Z}_p^*$

when $m=xp$: $(xp)^{\lambda(n)} \equiv (xp)^{\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}} \equiv (x^{p-1}p^{p-1})^{\frac{q-1}{\gcd(p-1,q-1)}} \equiv 1 \bmod p$

$(xp)^{\lambda(n)} \equiv (xp)^{\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}} \equiv (x^{q-1}p^{q-1})^{\frac{p-1}{\gcd(p-1,q-1)}} \equiv 1 \bmod q$

when $m=yq$: $(yq)^{\lambda(n)} \equiv (yq)^{\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}} \equiv (y^{p-1}q^{p-1})^{\frac{q-1}{\gcd(p-1,q-1)}} \equiv 1 \bmod p$

$(yq)^{\lambda(n)} \equiv (yq)^{\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}} \equiv (y^{q-1}q^{q-1})^{\frac{p-1}{\gcd(p-1,q-1)}} \equiv 1 \bmod q$

So any $m\in\mathbb{Z}_n$, $\begin{cases} m^{\lambda(n)} \equiv 1 \bmod p \\ m^{\lambda(n)} \equiv 1 \bmod q \end{cases}$ CRT $\Rightarrow m^{\lambda(n)} \equiv 1 \bmod n$

$m^{ed} \equiv m^{k\lambda(n)+1} \equiv [m^{\lambda(n)}]^k \cdot m \equiv m \bmod n$

So encryption and decryption are still inverse operations

$p=41 \quad q=37. \quad e=7$

$\lambda(n) = \frac{40\times 36}{\gcd(40,36)} = 360$

$ed \equiv 1 \bmod 360$.

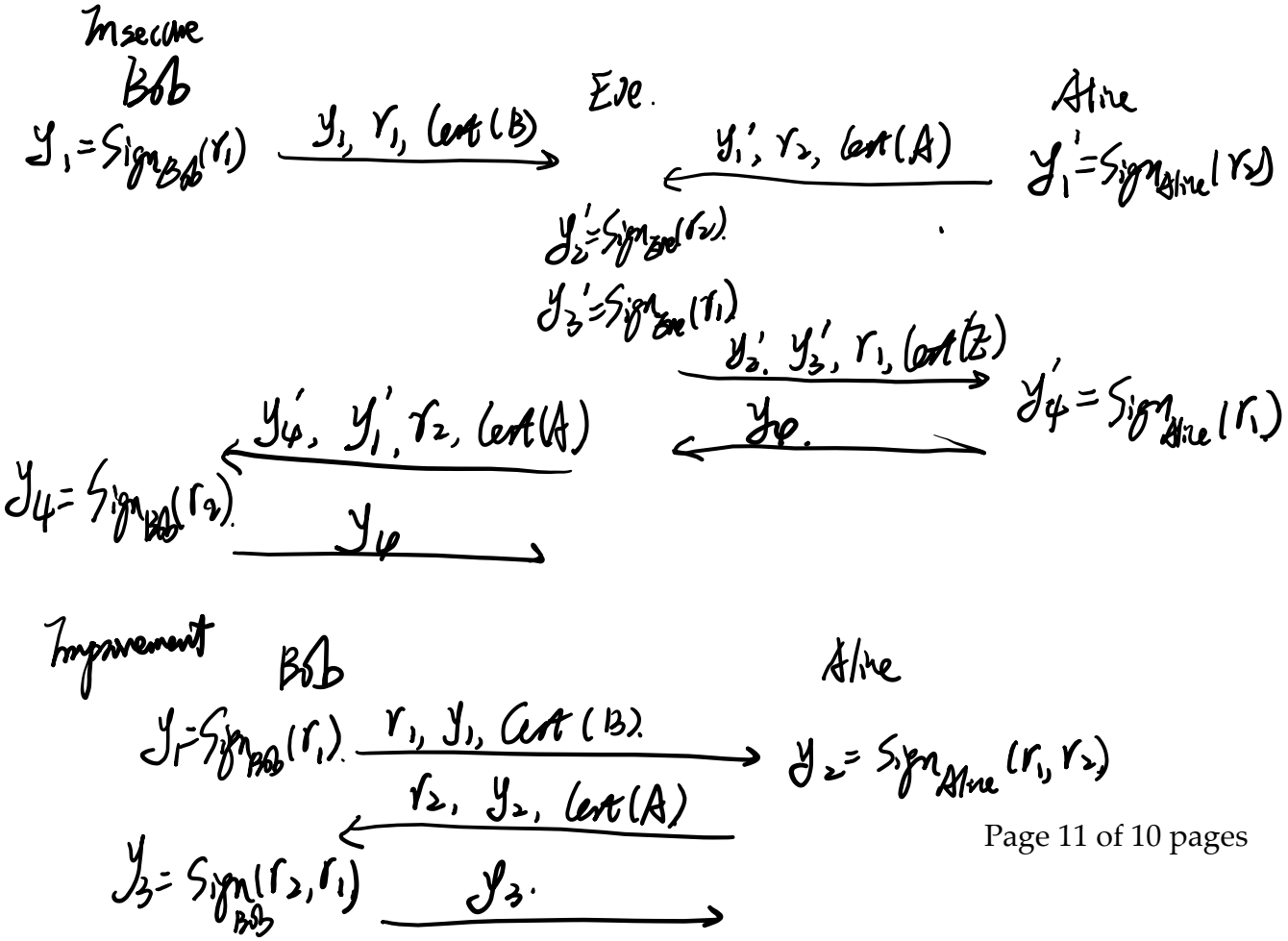
$d \equiv 7^{-1} \bmod 360$.

$d = 103$.

Q4. (10 marks) Consider the public-key mutual identification protocol presented in Protocol 1. Discuss whether Protocol 1 is secure. If it is secure, please give the security analysis; otherwise, please present the attack approach and improve it to be secure. Cert(Alice) is the public key certificate of Alice, and Cert(Bob) is the public key certificate of Bob. $sign_{Alice}(x)$ is Alice's signature of x, $verif_{Alice}(x, y)$ is the verification of y on x using Alice's public key. $sign_{Bob}(x)$ is Bob's signature of x, $verif_{Bob}(x, y)$ is the verification of y on x using Bob's public key.

Protocol 1: PUBLIC-KEY MUTUAL AUTHENTICATION

1. Bob chooses a random challenge, r_1. He also computes $y_1 = sign_{Bob}(r_1)$ and he sends Cert(Bob), r_1 and y_1 to Alice.
2. Alice verifies Bob's public key on the certificate Cert(Bob). Then she checks that $verif_{Bob}(r_1, y_1)$ = true. If not, then Alice "rejects" and quits. Otherwise, Alice chooses a random challenge, r_2. She also computes $y_2 = sign_{Alice}(r_1)$ and $y_3 = sign_{Alice}(r_2)$ and she sends Cert(Alice), r_2, y_2, and y_3 to Bob.
3. Bob verifies Alice's public key on the certificate Cert(Alice). Then he checks that $verif_{Alice}(r_1, y_2)$ = true and $verif_{Alice}(r_2, y_3)$ = true. If so, then Bob "accepts"; otherwise, Bob "rejects." Bob also computes $y_4 = sign_{Bob}(r_2)$ and he sends y_4 to Alice.
4. Alice checks that $verif_{Bob}(r_2, y_4)$ = true. If so, then Alice "accepts"; otherwise, Alice "rejects."



Q5. (10 marks) Suppose h_1: $\{0,1\}^{2m} \rightarrow \{0,1\}^m$ is a collision resistant hash function. Define h_2: $\{0,1\}^{6m} \rightarrow \{0,1\}^m$ as follows:

a. Write $x \in \{0,1\}^{6m}$ as $x = x_1 || x_2 || x_3$, where $x_1, x_2, x_3 \in \{0,1\}^{2m}$.

b. Define $h_2(x) = h_1(h_1(x_1) || h_1(x_2) || h_1(x_3))$.

Prove that h_2 is collision resistant.

assume that ~~h2 is collis~~

there is a collision on h_2.

this is, $x \neq x'$ $\quad x = x_1 || x_2 || x_3$ $\quad x' = x_1' || x_2' || x_3'$

$h_2(x) = h_2(x')$ $\quad h_2(x) = h_1(h_1(x_1) || h_1(x_2) || h_1(x_3))$

$\therefore h_1(h_1(x_1) || h_1(x_2) || h_1(x_3)) = h_1(h_1(x_1') || h_1(x_2') || h_1(x_3'))$

$\because$ h_1 is collision resistant

$\therefore h_1(x_1) || h_1(x_2) || h_1(x_3) = h_1(x_1') || h_1(x_2') || h_1(x_3')$ ①

$\therefore h_1(x_1) = h_1(x_1')$

$h_1(x_2) = h_1(x_2')$

$h_1(x_3) = h_1(x_3')$

and h_1 is collision resistant

$\therefore x_1 = x_1'$, $x_2 = x_2'$ $x_3 = x_3'$

$\therefore x = x'$ which ~~is~~ contradict with $x \neq x'$

$\therefore h_2$ is collision resistant.

Q6 (12 marks) Consider the digital signature scheme presented in Scheme 1.
a. What is the formula for verifying the signature $\sigma = (r, s)$?
b. Explain how an adversary can recover the secret key (i.e., x), when the signer, Alice, reuses the same random number k for two different messages. State your assumptions.
c. Assume the digital signature of message m is computed as follows: $[r, s] = [g^k \bmod p, H(m)(k - x \cdot r) \bmod p-1]$. Are there any security problems in the variant? If so, identify one and briefly justify it. If not, explain why not. (Note that in this question, you cannot assume that the signer will reuse the same random number k.)

Scheme 1. DIGITAL SIGNATURE - (Setup, KeyGen, Sign)
Setup: The shared global public parameters (p, g):
- choose a large prime p with $2^{L-1} < p < 2^L$, where L= 512 to 1024 bits and is a multiple of 64
- g is the generator of group Z_p.
- H is a cryptographic hash function: $\{0,1\}^* \rightarrow Z_{p-1}$

KeyGen: A user, Alice, chooses the private key x and computes the public key y:
- choose a random private key: $x \in Z_p$
- compute the public key: $y = g^x \bmod p$

Sign: to sign a message m, Alice:
- generate a random value $k \in Z_p$, k must be destroyed after use, and never be reused
- compute the signature pair: $r = g^k \bmod p$, $s = [k^{-1}(H(m) + x \cdot r)] \bmod p-1$
- send the signature $\sigma=(r, s)$ with message m

a.

$y = g^x$

compute $v = y^r = g^{xr} \bmod p$

$u = g^{H(m)} \bmod p$.

$t = v \cdot u \cdot g^{s^{-1}}$

to verify if t is ~~equal~~ equal to r

if $t = r$ the signature is valid.

else, the signature will be rejected.

(b) two different message m_1 and m_2.

$\sigma_1 = (r, s_1)$ $\sigma_2 = (r, s_2)$

$s_1 = [k^{-1}(H(m_1) + x \cdot r)] \bmod p-1$

$s_2 = [k^{-1}(H(m_2) + x \cdot r)]$.

$s_1, s_2, H(m_1), H(m_2)$, r is known.

k and x can be figured out through the two equation.

so the advarsary can get the secret key x

c. given (r, s) is the signature of a message m.
The adversary can computer $(r', s') = (r, sH(m)^{-1}h(m'))$, which is the signature of the message m'. So the adversary succeeds to generate a forge.