Cybersecurity/CNS
January 19, 2024

1. Hashing (5)

Is a strongly resistant hashing function also weakly resistant?	Y	N
Is a weakly resistant hashing function also strongly resistant?	Y	N
Are unkeyd hashing functions more secure than keyed hashing functions?	Y	N
F1 is an n-bit range hashing function. F2 is another hashing function with k-bit range, $k < n$. Is the total number of collisions of F1(F2(x)) greater than that of F2(F1(x)), for $x \in (0+1)^*$?	Y	N
$H(x) = x^2$. Is H(x) cryptographics?	Y	N

2. Digital signatures (5)

2.1. Conceptually describe the process of putting an RSA digital signature on a pdf document. Include verification. (2)

2.2. ElGamal signature vs. DSS (draw a table and be schematic) (1)

2.3. How to use a digital signature for authentication, being robust against the replay attack? (2)

3. Symmetric encryption (6)

3.1. Given a cipher algorithm A, why 2-A (encrypting again the cipher text of A) is not much more secure than A?(1)

3.2. Explain why it is bad to reuse the same keystream in OTP (1)

3.3. What does the command "openssl aes-128-cbc -p -in file.txt -out file.txt.enc" produce? Describe in detail, also analysing the output format. (2.5)

3.4. Give two reasons why it is not a good idea to encrypt a file through a cryptographic hashing function (1.5)

4. iptables (6)

4.1. How to set a default "white list" policy on a chain? (1)

4.2. What is the effect of the following iptables command?

```
iptables -I INPUT -p tcp  --dport 1024:65535 --sport 0:1023 -i lo -j DROP
```

Carefully describe it. (2)

4.3. Write the appropriate iptables commands used for personal firewalls, which block (bidirectional) communications with the host 192.168.7.2 initiated by the host but allow those (still bidirectional) initiated by localhost. The default is blacklisting. (3)

5. Authentication (7)

5.1. Authentication done over the Internet without special care could be attacked with a replay attack. Give at least two examples (2)

5.2. What can you do to make the examples in the previous step safe? (2)

5.3. What are the rainbow tables and why are they dangerous? (1.5)

5.4. Describe what an offline dictionary attack on the passwords is. (1.5)

6. Short questions (4)

6.1. Show how to manually compute $2^{100} \bmod 7$ (1)

continues →

6.2. TLS vs IPsec (draw a table). (2)
6.3. Define what a perfect cipher is. (1)

Write number of 2023 homeworks that have been delivered

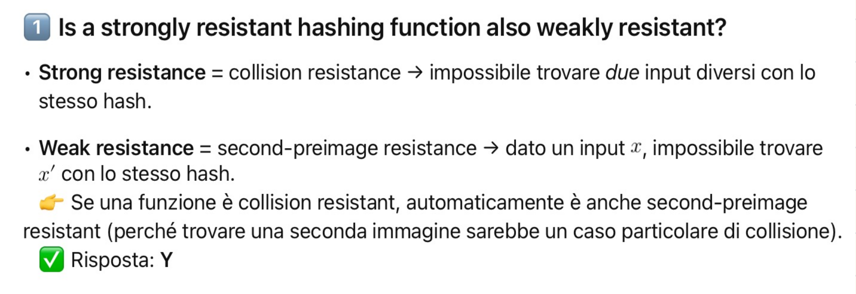
____

Signature

____

continues →

1 a

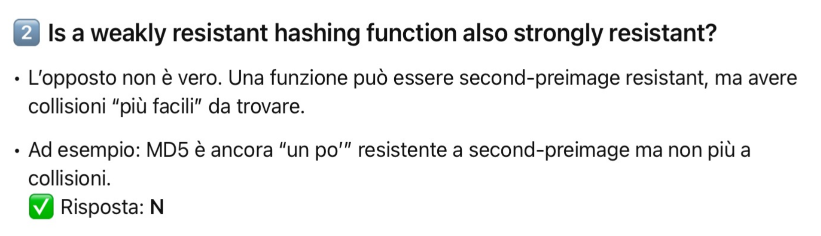


1️⃣ **Is a strongly resistant hashing function also weakly resistant?**

- **Strong resistance** = collision resistance → impossibile trovare *due* input diversi con lo stesso hash.
- **Weak resistance** = second-preimage resistance → dato un input x, impossibile trovare x' con lo stesso hash.

👉 Se una funzione è collision resistant, automaticamente è anche second-preimage resistant (perché trovare una seconda immagine sarebbe un caso particolare di collisione).
✅ Risposta: **Y**

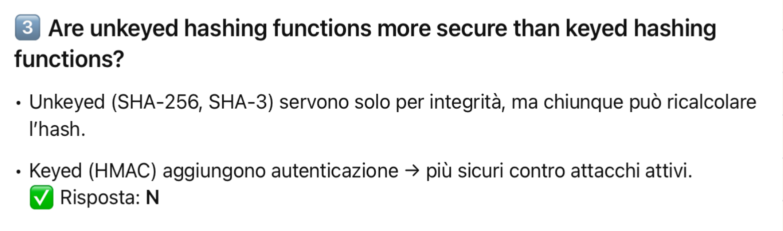
b



2️⃣ **Is a weakly resistant hashing function also strongly resistant?**

- L'opposto non è vero. Una funzione può essere second-preimage resistant, ma avere collisioni "più facili" da trovare.
- Ad esempio: MD5 è ancora "un po'" resistente a second-preimage ma non più a collisioni.
✅ Risposta: **N**

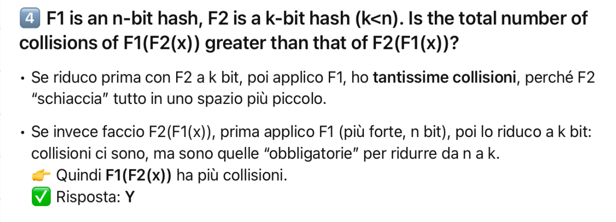
c



3️⃣ **Are unkeyed hashing functions more secure than keyed hashing functions?**

- Unkeyed (SHA-256, SHA-3) servono solo per integrità, ma chiunque può ricalcolare l'hash.
- Keyed (HMAC) aggiungono autenticazione → più sicuri contro attacchi attivi.
✅ Risposta: **N**

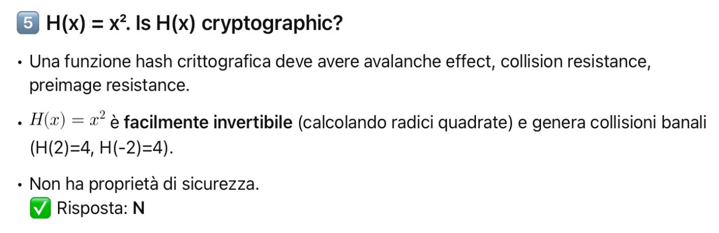
d



4️⃣ **F1 is an n-bit hash, F2 is a k-bit hash (k<n). Is the total number of collisions of F1(F2(x)) greater than that of F2(F1(x))?**

- Se riduco prima con F2 a k bit, poi applico F1, ho **tantissime collisioni**, perché F2 "schiaccia" tutto in uno spazio più piccolo.
- Se invece faccio F2(F1(x)), prima applico F1 (più forte, n bit), poi lo riduco a k bit: collisioni ci sono, ma sono quelle "obbligatorie" per ridurre da n a k.
👉 Quindi **F1(F2(x))** ha più collisioni.
✅ Risposta: **Y**

e



5️⃣ **H(x) = x². Is H(x) cryptographic?**

- Una funzione hash crittografica deve avere avalanche effect, collision resistance, preimage resistance.
- $H(x) = x^2$ è **facilmente invertibile** (calcolando radici quadrate) e genera collisioni banali (H(2)=4, H(-2)=4).
- Non ha proprietà di sicurezza.
✅ Risposta: **N**

2.1 THE SIGNER FIRST COMPUTES THE HASH OF THE DOCUMENT. THE DIGEST IS THEN ENCRYPTED WITH THE SIGNER'S PRIV KEY, PRODUCING THE DIGITAL SIGNATURE, WHICH IS ATTACHED TO THE PDF TOGETHER WITH THE SIGNER'S PUBLIC KEY.
THE RECIPIENT RECOMPUTES THE HASH OF THE PDF, THEN DECRYPTS THE DIGITAL SIGNATURE WITH THE SIGNER'S PUBLIC KEY. IF BOTH HASHES MATCH THE SIGNATURE IS VALID.

2.2

	ELGAMAL	DSS
KEYS	LONG TERM PRIV KEY + RANDOM K	SAME
SIGN SIZE	TWO LARGE INT	(r,s) SMALLER
EFFICIENCY	LESS EFFICIENT	MORE EFFICIENT
STANDARDIZATION	NOT STANDARDIZED	STANDARDIZED

2.3 DURING LOGIN, THE SERVER GENERATES A RANDOM CHALLENGE (NONCE) AND SENDS IT TO THE CLIENT. THE CLIENT SIGNS THE CHALLENGE TOGETHER WITH ITS IDENTITY USING ITS PRIVATE KEY AND RETURNS THE SIGNATURE. THE SERVER VERIFIES THE SIGNATURE WITH THE CLIENT'S PUB KEY.
BECAUSE EACH CHALLENGE IS UNIQUE AND USED ONLY ONCE, AN ATTACKER CANNOT REUSE AN OLD SIGNED MESSAGE TO GAIN ACCESS.

3.1 BECAUSE OF THE MEET IN THE MIDDLE, IN DOUBLE ENCRYPTION THE ATTACKER CAN ENCRYPT FROM ONE SIDE AND DECRYPT FROM THE OTHER, STORING INTERMEDIATE VALUES, AND MATCH THEM IN 2^n STEPS INSTEAD OF 2^{2n} FOR AN n-BIT KEY.

3.2 IF THE SAME KEYSTREAM IS REUSED TO ENCRYPT TWO MESSAGES m_1 & m_2, THE CIPHERTEXTS $c_1 = m_1 \oplus k$ AND $c_2 = m_2 \oplus k$ CAN BE COMBINED:

$$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

3.3 THE COMMAND ENCRYPTS FILE.TXT IN INPUT WITH AES-128 IN CBC MODE USING A PASSPHRASE (PROMPTED). THE ENCRYPTED FILE IS THE OUTPUT.

3.4 AN HASH FUNCTION IS ONE-WAY AND CANNOT BE INVERTED, SO ONCE A FILE IS HASHED THE ORIGINAL CONTENT IS IRRECOVERABLE. IN ADDITION, HASHING ALWAYS PRODUCES A FIXED-LENGTH DIGEST THAT DISCARDS MOST OF THE INFORMATION IN THE FILE.
ENCRYPTION MUST ALLOW BOTH CONFIDENTIALITY AND DECRYPTION, WHILE HASHING ONLY PROVIDES INTEGRITY.

4.1 THE DEFAULT POLICY IS DROP: `IPTABLES -P <CHAIN> DROP`

4.2 THE COMMAND BLOCKS ALL INCOMING TCP PACKETS ON THE LOOPBACK INTERFACE WHOSE DESTINATION PORT IS IN THE RANGE 1024-65535 AND WHOSE SOURCE PORT IS IN THE PRIVILEGED RANGE 0-1023.

4.3
```
IPTABLES -A INPUT -i lo -j ACCEPT
IPTABLES -A OUTPUT -o lo -j ACCEPT

IPTABLES -A INPUT -m CONNTRACK --CTSTATE ESTABLISHED,RELATED -j ACCEPT
IPTABLES -A OUTPUT -m CONNTRACK --CTSTATE ESTABLISHED,RELATED -j ACCEPT

IPTABLES -A INPUT -S 192.168.7 2 -m CONNTRACK --CTSTATE NEW -j DROP
```

5.1 AN ADVERSARY CAN CAPTURE VALID CREDENTIALS AND REUSE THEM LATER.
IF A CLIENT SIMPLY SENDS ITS USERNAME AND PASSWORD OVER AN ENCRYPTED CHANNEL ONCE, AN ATTACKER WHO RECORDS THE EXCHANGE CAN REPLAY THE SAME LOGIN MESSAGE TO GAIN ACCESS.
IF AUTHENTICATION IS BASED ON SENDING A STATIC DIGITAL SIGNATURE ON A FIXED CHALLENGE OR TIMESTAMP, THE ATTACKER CAN CAPTURE AND RESEND IT WITHOUT NEEDING THE PRIV KEY.

5.2 THE SOLUTION IS TO ADD ALWAYS A DIFFERENT NONCE FOR EACH DIGITAL SIGNATURE. THUS WHEN THE ATTACKER CAPTURE THE SIGNATURE HE CAN'T RESEND IT BECAUSE THE NONCE IS EXPIRED.

5.3 THEY ARE LARGE PRECOMPUTED TABLES THAT MAP PLAINTEXT PASSWORDS TO THEIR HASH VALUES. THEY ARE USED BY ATTACKERS TO REVEASE HASH FUNCTIONS: INSTEAD OF BRUTE FORCING EVERY POSSIBLE PASSWORD ONLINE, THE ATTACKER COMPUTES HASHES IN ADVANCE AND LATER LOOKS UP THE HASH FOUND IN A PASSWORD DB TO RECOVER THE ORIGINAL PASSWORD.
MANY SYSTEMS USED TO STORE ONLY UNSALTED HASHES, SO THE SAME PASSWORD PRODUCES THE SAME DIGEST.

5.4 THIS ATTACK CONSISTS OF TESTING CANDIDATE PASSWORDS AGAINST STORED PASSWORD HASHES WITHOUT INTERACTING WITH THE SYSTEM.

1. OBTAIN THE PASSWORD DB
2. FOR EACH CANDIDATE PASSWORD p IN A DICTIONARY OF COMMON PASSWORDS:
   a IF A SALT IS USED, COMBINE p WITH THE CORRESPONDING SALT
   b COMPUTE THE HASH OF THE CANDIDATE
   c COMPARE THE RESULT WITH THE STORED HASH
3 IF A MATCH IS FOUND, p IS THE RECOVERED PASSWORD

SINCE THIS IS DONE OFFLINE, THE ATTACKER CAN TRY MANY TIMES WITHOUT BEING DETECTED.

6.1 $2^{100} \bmod 7 \rightarrow a^{p-1} = 1 \pmod{p} \longleftarrow$ IF p IS PRIME AND a IS NOT MULTIPLE OF p

$2^{6} = 1 \pmod{7} \longrightarrow 100 = 6 \cdot 16 + 4 \longrightarrow 2^{100} = 2^{4} \pmod{7}$

$2^{100} = 16 \pmod{7} \rightarrow 2^{100} = 2 \pmod{7}$

6.2

	TLS	IPSEC
LAYER	TRANSPORT	NETWORK
SCOPE	SECURE SPECIFIC APPLICATIONS (HTTPS, SMTP, IMAPS)	SECURE ALL IP TRAFFIC BETWEEN HOST /NETWORK
KEY MANAGEMENT	USES HANDSHAKE WITH CERTIFICATES	USES IKE PROTOCOL
TYPICAL USE	SECURE WEB, EMAIL, VPN OVER SSL	VPN, SITE TO SITE TUNNELS, HOST TO HOST SECURITY
DEPLOYMENT COMPLEXITY	EASIER	MORE COMPLEX

6.3 A PERFECT CIPHER IS ONE THAT PROVIDES PERFECT SECRECY, MEANING THE CIPHERTEXT REVEALS NO INFORMATION ABOUT THE PLAINTEXT.
AN EXAMPLE IS ONE TIME PAD (OTP).