| | | |
|---|---|---|
| Name: | Last name: | Id: |

**Cybersecurity**
**Computer and network security**
**Sicurezza nelle reti e nei sistemi informatici**
**Crittografia e sicurezza delle reti**

*Exam of July 14th, 2023. Time: 2 hours*

1. ***Please fill & sign this form, to be consigned to the prof.***
2. ***FOR NON-ENGLISH: 2 penalty points (only applicable to English courses)***
3. ***FOR UNREADABLE HAND-WRITING: discretionary decision***
4. ***YOU ARE KINDLY REQUESTED NOT TO WRITE BY A PENCIL. BALLPOINT PENS ARE STRONGLY PREFERRED***

Q1: **About hashing**
Evaluate the truth of the following assertions (please mark by **X** the T or F column, for true or alse). [correct: +0.5; wrong: -0.25; no answer: 0]

| Assertion | T | F |
|---|---|---|
| Strongly resistant hashing functions are also weakly resistant | | |
| is well-known that weak resistance implies strong resistance | | |
| cryptographic hashing function is a good candidate as a one-way function | | |
| yptographic hashing functions can be used as encryptors | | |
| e birthday attack is useless against strongly resistant hashing functions | | |
| yed hashing functions are robust wrt the birthday attack | | |
| ital signature operations are based on keyed hashing | | |
| A-1 has been obsoleted | | |
| en a pair ($m$, H($m$)), where $m$ is a message and H is a hashing function, irthday attack can help to find a colliding message $m' \neq m$ | | |
| day attacks have polynomial time complexity | | |

**Digital signatures**

2.1 [3/30] Define what a forgery attack is and describe the types of forgery attacks that can be made against digital signatures, also discussing their strength.

2.2 [4/30] Provide the broad outlines of both RSA and DSA, making a comparison between the two approaches.

2.3 [4/30] Alice and Bob want to digitally sign a contract D. Discuss and compare the two following approaches:

- Alice computes Sign$_A$(D), her digital signature of D, and sends to Bob (D, Sign$_A$(D)). Similarly, Bob sends to Alice (D, Sign$_B$(D)).
- Alice sends to Bob (D, Sign$_A$(D)); then Bob sends to Alice (D||Sign$_A$(D), Sign$_B$(D||Sign$_A$(D)), where symbol || denotes concatenation.

**ec and its infrastructure**

1 [3/30] Provide a *black-box* description of IPSec (non black-box descriptions will be considered as errors).

|  |  |  |
|---|---|---|
| Name: | Last name: | Id: |

Q3.2 [2/30] Provide two use cases of IPSec.

Q3.3 [2/30] Alice needs to send a confidential file to Bob. Can you imagine a case where Alice will have to use both IPSec and TLS?

Q4: **Iptables**

Your host is acting as a firewall protecting your private network; the Internet is connected to the firewall interface `eth0`, while the private network is connected to the firewall interface `eth1`. Default policies are based on blacklisting.

Q4.1 [3/30] You want to protect your local web server located at IP 192.168.13.80 by adding a rule that allows public IP 201.202.203.204 making `http` connections to the web server, but no more than 2 per second. Write an `iptables` command line adding such a rule to the proper chain.

Q4.2 [2/30] Write two `iptables` emergency rules blocking all incoming traffic (from Internet to private network) and all outgoing traffic (from private network to Internet).

Q4.3 [2/30] Block `ssh` traffic to `iptable` host.

Q5: **Short question (You have to show your ability to be concise)**

Provide short answers to the following questions.

Q5.1 [2/30] Use Bézout's identity for computing the inverse multiplicative of 19 mod 37. (No scientific calculator allowed!)

***VE YOU SENT 2022-23 HOMEWORKS TO THE PROF.? YES / [✓ NO] (circle your answer)***

*ES:*

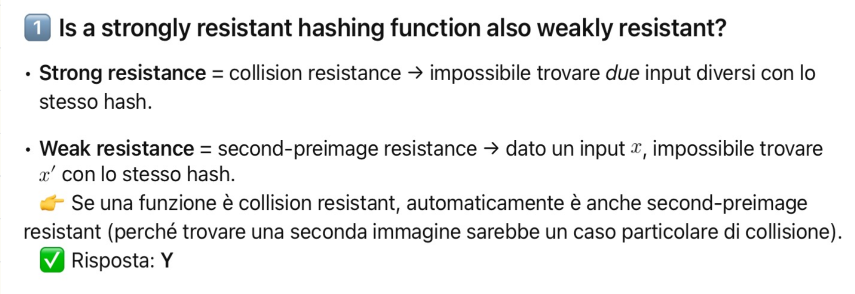
*reby confirm that I sent no. ______________ contributions*

*Signature*

______________________________

*e sign, in case of both yes and no!)*

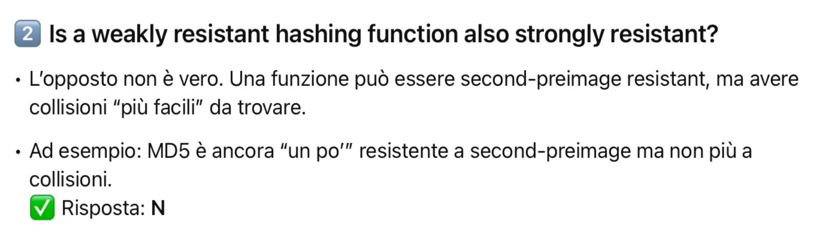
1.1 T



### 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**

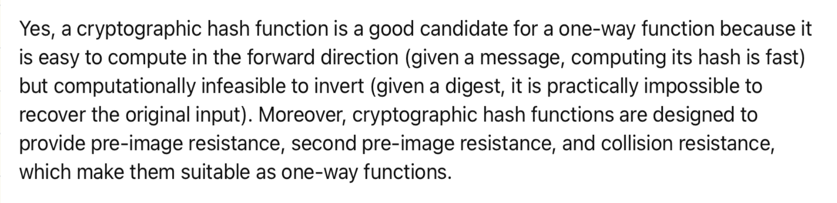
1.2 F



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

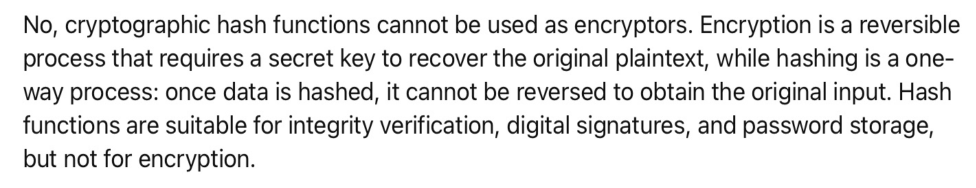
- L'opposto non è vero. Una funzione può essere second-preimage resistant, ma avere collisioni "più facili" da trovare.
- Ad esempio: MD5 è ancora "un po'" resistente a second-preimage ma non più a collisioni.
  ✅ Risposta: **N**

1.3 T



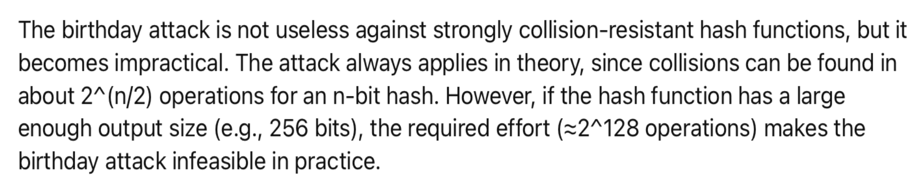
Yes, a cryptographic hash function is a good candidate for a one-way function because it is easy to compute in the forward direction (given a message, computing its hash is fast) but computationally infeasible to invert (given a digest, it is practically impossible to recover the original input). Moreover, cryptographic hash functions are designed to provide pre-image resistance, second pre-image resistance, and collision resistance, which make them suitable as one-way functions.

1.4 F



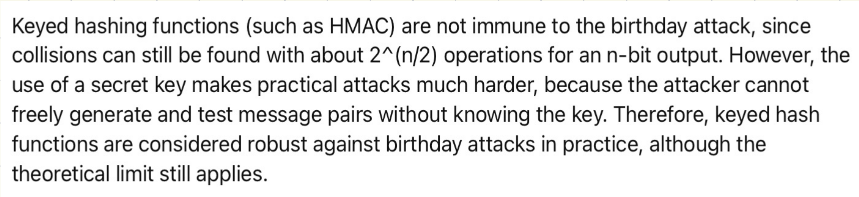
No, cryptographic hash functions cannot be used as encryptors. Encryption is a reversible process that requires a secret key to recover the original plaintext, while hashing is a one-way process: once data is hashed, it cannot be reversed to obtain the original input. Hash functions are suitable for integrity verification, digital signatures, and password storage, but not for encryption.

1.5 F



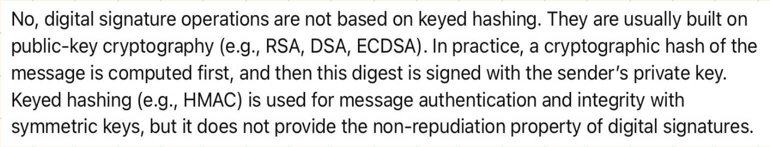
The birthday attack is not useless against strongly collision-resistant hash functions, but it becomes impractical. The attack always applies in theory, since collisions can be found in about 2^(n/2) operations for an n-bit hash. However, if the hash function has a large enough output size (e.g., 256 bits), the required effort (≈2^128 operations) makes the birthday attack infeasible in practice.

1.6 T



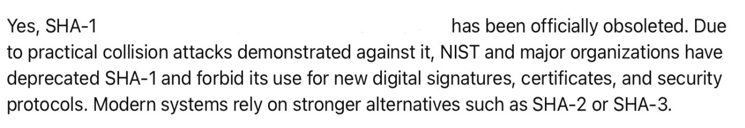
Keyed hashing functions (such as HMAC) are not immune to the birthday attack, since collisions can still be found with about 2^(n/2) operations for an n-bit output. However, the use of a secret key makes practical attacks much harder, because the attacker cannot freely generate and test message pairs without knowing the key. Therefore, keyed hash functions are considered robust against birthday attacks in practice, although the theoretical limit still applies.

1.7 F



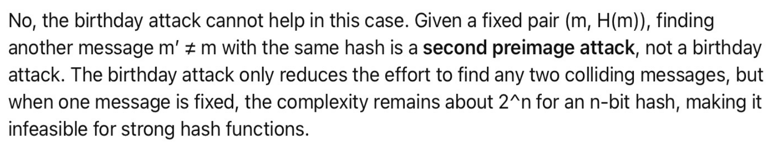
No, digital signature operations are not based on keyed hashing. They are usually built on public-key cryptography (e.g., RSA, DSA, ECDSA). In practice, a cryptographic hash of the message is computed first, and then this digest is signed with the sender's private key. Keyed hashing (e.g., HMAC) is used for message authentication and integrity with symmetric keys, but it does not provide the non-repudiation property of digital signatures.

1.8 T



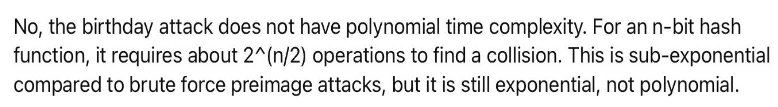
Yes, SHA-1 has been officially obsoleted. Due to practical collision attacks demonstrated against it, NIST and major organizations have deprecated SHA-1 and forbid its use for new digital signatures, certificates, and security protocols. Modern systems rely on stronger alternatives such as SHA-2 or SHA-3.

1.9 F



No, the birthday attack cannot help in this case. Given a fixed pair (m, H(m)), finding another message m' ≠ m with the same hash is a **second preimage attack**, not a birthday attack. The birthday attack only reduces the effort to find any two colliding messages, but when one message is fixed, the complexity remains about 2^n for an n-bit hash, making it infeasible for strong hash functions.

1.10 F



No, the birthday attack does not have polynomial time complexity. For an n-bit hash function, it requires about 2^(n/2) operations to find a collision. This is sub-exponential compared to brute force preimage attacks, but it is still exponential, not polynomial.

2.1 A FORGERY ATTACK AGAINST A DIGITAL SCHEME IS AN ATTEMPT BY AN ADVERSARY TO PRODUCE A VALID SIGNATURE WITHOUT KNOWING THE KEY:

EXISTENTIAL: THE ATTACKER PRODUCES AT LEAST ONE VALID MESSAGE-SIGNATURE PAIR, EVEN IF THE MESSAGE HAS NO PARTICULAR MEANING

SELECTIVE: THE ATTACKER CAN FORGE A VALID SIGNATURE FOR A SPECIFIC CHOSEN MESSAGE

UNIVERSAL: THE ATTACKER CAN FORGE VALID SIGNATURES FOR ANY MESSAGES

2.2 RSA IS A PUB KEY SCHEME BASED ON THE HARDNESS OF INTEGER FACTORIZATION. KEY GENERATION SELECTS TWO LARGE PRIMES AND PRODUCES A MODULUS $n$. A PRIV EXPONENT $d$ AND PUB EXPONENT $e$ ARE COMPUTED. FOR SIGNATURES, THE MESSAGE DIGEST IS RAISED TO $d$ MOD $n$, AND VERIFICATION USING $e$.

DSA IS BASED ON THE DISCRETE LOGARITHM PROBLEM IT USES GROUP PARAMETERS $(p, q, g)$, A PRIV KEY $x$, AND A PUB KEY $y = g^x \bmod p$. FOR EACH SIGNATURE, A FRESH RANDOM VALUE $k$ IS USED TO PRODUCE A PAIR $(r, s)$. VERIFICATION USES THE SIGNER'S PUB KEY.

RSA IS VERSATILE AND WIDELY DEPLOYED, USABLE FOR BOTH ENC AND SIGN, BUT GENERALLY REQUIRES LONGER KEYS AND SLOWER SIGNING
DSA IS SIGNATURE SPECIFIC, MORE EFFICIENT IN SIGNING BUT SLOWER IN VERIFICATION.

2.3 a THIS ENSURES BOTH PARTIES HAVE SIGNED D, BUT THE SIGNATURES ARE INDEPENDENT. THERE IS NO CRYPTOGRAPHIC BINDING BETWEEN THEM, SO A SIGNATURE COULD POTENTIALLY BE REUSED IN ANOTHER CONTEXT.

b NOW THE SIGNATURES ARE CHAINED BECAUSE BOB'S SIGNATURE CERTIFIES NOT ONLY THE CONTRACT BUT ALSO ALICE'S SIGNATURE. THUS THE TWO SIGNATURES CANNOT BE SEPARATED OR REUSED INDIPENDENTLY.

3.1 IPSEC CAN BE DESCRIBED AS A BLACK BOX THAT TAKES STANDARD IP PACKETS AS INPUT AND PRODUCES SECURE IP PACKETS AS OUTPUT. IT PROVIDES:

CONFIDENTIALITY BY ENCRYPTING THE PAYLOAD
INTEGRITY AND AUTHENTICATION
REPLAY PROTECTION TO PREVENT REUSE OF OLD PACKETS

3.2 a REMOTE ACCESS VPN: A REMOTE EMPLOYEE SECURELY CONNECTS TO THE CORPORATE NETWORK OVER THE INTERNET USING IPSEC.

b SITE TO SITE VPN. TWO COMPANY OFFICES USE IPSEC TUNNELS BETWEEN THEIR ROUTERS OR FIREWALLS TO PROTECT ALL INTER SITE COMMUNICATIONS.

33 SUPPOSE ALICE CONNECTS REMOTELY TO BOB'S CORPORATE NETWORK THROUGH AN IPSEC VPN, WHICH SECURES THE CHANNEL BETWEEN HER DEVICE AND THE COMPANY GATEWAY. WITHIN THIS TUNNEL, SHE THEN USES TLS TO TRANSFER THE CONFIDENTIAL FILE DIRECTLY TO BOB'S SERVER. IPSEC ENSURES SECURE NETWORK LEVEL COMMUNICATION, WHILE TLS PROVIDES END-TO-END PROTECTION AT THE APPLICATION LEVEL.

4.1
```
IPTABLES -A FORWARD -p TCP -S 201.202.203.204 -d 192.168.13.80
--DPORT 80 -m LIMIT --LIMIT 2/SECOND -j ACCEPT
```

4.2
```
IPTABLES -A FORWARD -i eth0 -o eth1 -j DROP
IPTABLES -A FORWARD -i eth1 -o eth0 -j DROP
```

4.3
```
IPTABLES -A INPUT -p TCP --DPORT 22 -j DROP
```

5.1 $19 \bmod 37 \rightarrow \quad 19x = 1 \bmod 37$

$37 = 1 \cdot 19 + 18 \qquad (18 = 37 - 19)$

$19 = 1\ 18 + 1 \qquad (1 = 19 - 18)$

$\downarrow$

$1 = 19 - (37 - 19)$

$1 = 19 - 37 + 19$

$1 = 2 \cdot 19 - 37$

$1 = 2 \cdot 19 - 1 \cdot 37$

$\downarrow$

$2 \cdot 19 = 1 \bmod 37$

$\downarrow$

$19^{-1} = 2 \bmod 37$