9️⃣

Exercise 9

💡 **Reading material (optional)**
[1] For recent attacks on DKIM, see Chen, Paxson, Jiang, "Composition Kills: A Case Study of Email Sender Authentication" (2020).https://www.usenix.org/system/files/sec20-chen-jianjun.pdf
[2] Email forwarding chain attacks and verification using DKIM, SPF, and DMARC, can be found in Shen et al, "Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks" (2021)https://www.usenix.org/system/files/sec21summer_shen-kaiwen.pdf

DKIM verification tasks

View the email spam.eml.

Frage 1

In which lines is the DKIM signature header located? Specify all line numbers individually in ascending order, separated by commas.

> Antwort:
> `41,42,43`

Frage 2

Which lines of the header, other than the DKIM signature itself, are protected by the DKIM signature? Specify all line numbers individually in ascending order, separated by commas.

> Antwort:
> `53,54,55,56,58`

h=To:Cc:From:Subject:Date:From;

Frage 3

Which algorithm was used to generate the DKIM signature? Specify the algorithm as it is specified in the DKIM standard.

> Antwort:
> `rsa-sha256`

Frage 4

What is the header canonicalization method used in DKIM signature?

> Wählen Sie eine Antwort:
>
> ☑ ~~relaxed~~
>
> ☐ simple

Frage 5

What is the body canonicalization method used in the DKIM signature?

> Wählen Sie eine Antwort:
>
> ☐ relaxed
>
> ☑ ~~simple~~

Frage 6

What is the body hash specified in the DKIM signature? Specify the result as a complete hash value in hexadecimal, including leading zeros.

> Antwort:
> `0x06ff15ec64fe38fd24b9a49b0fc768d14ccb464fa8f92acc475c50a771f85740`

```
bh=Bv8V7GT+OP0kuaSbD8do0UzLRk+o+SrMR1xQp3H4V0A=;

anakles@NB-XPS:~$ echo 'Bv8V7GT+OP0kuaSbD8do0UzLRk+o+SrMR1xQp3H4V0A=' | base64 -d > dkim_hex
anakles@NB-XPS:~$ xxd dkim_hex

00000000: 06ff 15ec 64fe 38fd 24b9 a49b 0fc7 68d1  ....d.8.$.....h.
00000010: 4ccb 464f a8f9 2acc 475c 50a7 71f8 5740  L.FO..*.G\P.q.W@

0x06ff15ec64fe38fd24b9a49b0fc768d14ccb464fa8f92acc475c50a771f85740
```

Frage 7

What is the body from which the body hash was calculated in its canonicalized form? In the solution, specify the characters Carriage Return (ASCII 0x0d) as '\r' and Linefeed (ASCII 0x0a) as '\n'.

> Antwort:
> `\r\nWe have the best conserved ham on the market! Low prices and great\r\navailability. Buy fast, buy often!`

```
We have the best conserved ham on the market! Low prices and great
availability. Buy fast, buy often!
```

Frage 8

Which domain name do you need to query to find the DKIM signature public key?

> Antwort:
> `rub.de`

Frage 9

Which domain record type do you need to query to retrieve the DKIM signature public key?

> Antwort:
> `mail-2017`

Frage 10

Get the DKIM DNS record matching the DKIM signature in the email. This contains the public RSA key for the signature in an ASN.1 data structure. However, this is in turn encapsulated as a bit string in a higher-level ASN.1 data structure. For example, you can use the following online tool to parse this structure: https://lapo.it/asn1js/.

What is the RSA modulus used in hexadecimal?

> Antwort:
> `0x5b8e9197201d654bc2c674ba3ff23bb833f95ee719393d0a535082c9f`

https://easydmarc.com/tools/dkim-lookup?domain=rub.de&selector=mail-2017

```
v=DKIM1; h=sha256; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDbsTHlwVHjoU6HyBjult6Q8xh65hUFtku2EEkf1ubgzAQf0tly4KseikeNNbHG32ICUmaF7liwTk7D4c


SEQUENCE (2 elem)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
    NULL
  BIT STRING (1120 bit) 001100001000000110001001000000101000000110000001000000001101101110110…
    SEQUENCE (2 elem)
      INTEGER (1024 bit) 154273086532317434646205966737168466430676300936500873872409188904095…
      INTEGER 65537
```

```
>>> hex(154273086532317434646205966737168466430676300936500873872409188904095)
'0x5b8e9197201d654bc2c674ba3ff23bb833f95ee719393d0a535082c9f'
```

Frage 11

What is the public RSA exponent (in decimal)?

> Antwort:
> `65537`

Frage 12

Now calculate the message signed by the email server from the DKIM signature by exponentiating the value of the signature with the public RSA exponent (modulus the public RSA modulus). You can use the Python function pow(basis, exponent, modulus) to do this.
Represent the result as a hexadecimal number and specify the lower 32 bytes.

> 💡 *Note*: If you have solved the task correctly, the upper bytes of the message are "00 01 ff ff ff ...". This corresponds to the PKCS #1 v1.5 padding. The lower 32 bytes are then the hash value of the DKIM header data (see the following task).

> Antwort:

Frage 13

The DKIM header data is formed as follows:
(1) The algorithm starts with the empty output string R and the complete e-mail
E with the DKIM signature parameter h=H_0:H_1:...:H_n. Repeat the following step (2) for i=0...n and then go to step (3).

(2) Search backwards in the e-mail E for the header H := H_i. If no such header (more) exists, skip this step. Otherwise, let H' be the canonicalized form of H (according to the rules required in the DKIM header). Then substitute
R := R | H' | CRLF
E := E - H

where "|" is the concatenation of strings, CRLF is the string consisting of carriage return and linefeed (0x0d, 0x0a), and E-H is the result of deleting header H from email E.

(3) Find the DKIM signature header in E and remove from it the value of the parameter b= (i.e., replace "b=XY...Z" with "b="). Call the result D and replace
R := R | D

Note: No CRLF is appended in this step.

(4) Return R. This string contains the DKIM header data.

What is the full DKIM header data of the email spam.eml under the included DKIM policy? In the solution, specify the characters Carriage Return (ASCII 0x0d) as '\r' and Linefeed (ASCII 0x0a) as '\n'.

Note : You can check yourself by forming the hash value of the DKIM header data. This must match the value from task 12. The last two bytes of the hash value are 0x5c40.

> Antwort:

Frage 14

Does the DKIM policy included in the email prevent an attacker from changing the existing Cc header (except for canonicalization) without being noticed?

> Antwort:
>
> ☑ ~~Yes~~
>
> ☐ No

Frage 15

Does the DKIM policy included in the email prevent an attacker from deleting the existing Cc header unnoticed?

> Antwort:
>
> ☑ ~~Yes~~

- [ ] No

Frage 16

Does the DKIM policy included in the email prevent an attacker from adding another Cc header undetected?

Wählen Sie die richtige(n) Antwort(en) aus:

- [x] ~~No, if the attacker inserts the header after the existing Cc header~~
- [ ] Yes, no matter where the attacker inserts the header
- [ ] No, if the attacker inserts the header before the existing Cc header

Frage 17

Does the DKIM policy included in the email prevent an attacker from adding another From header undetected?

Antwort:

- [x] ~~Yes~~
- [ ] No