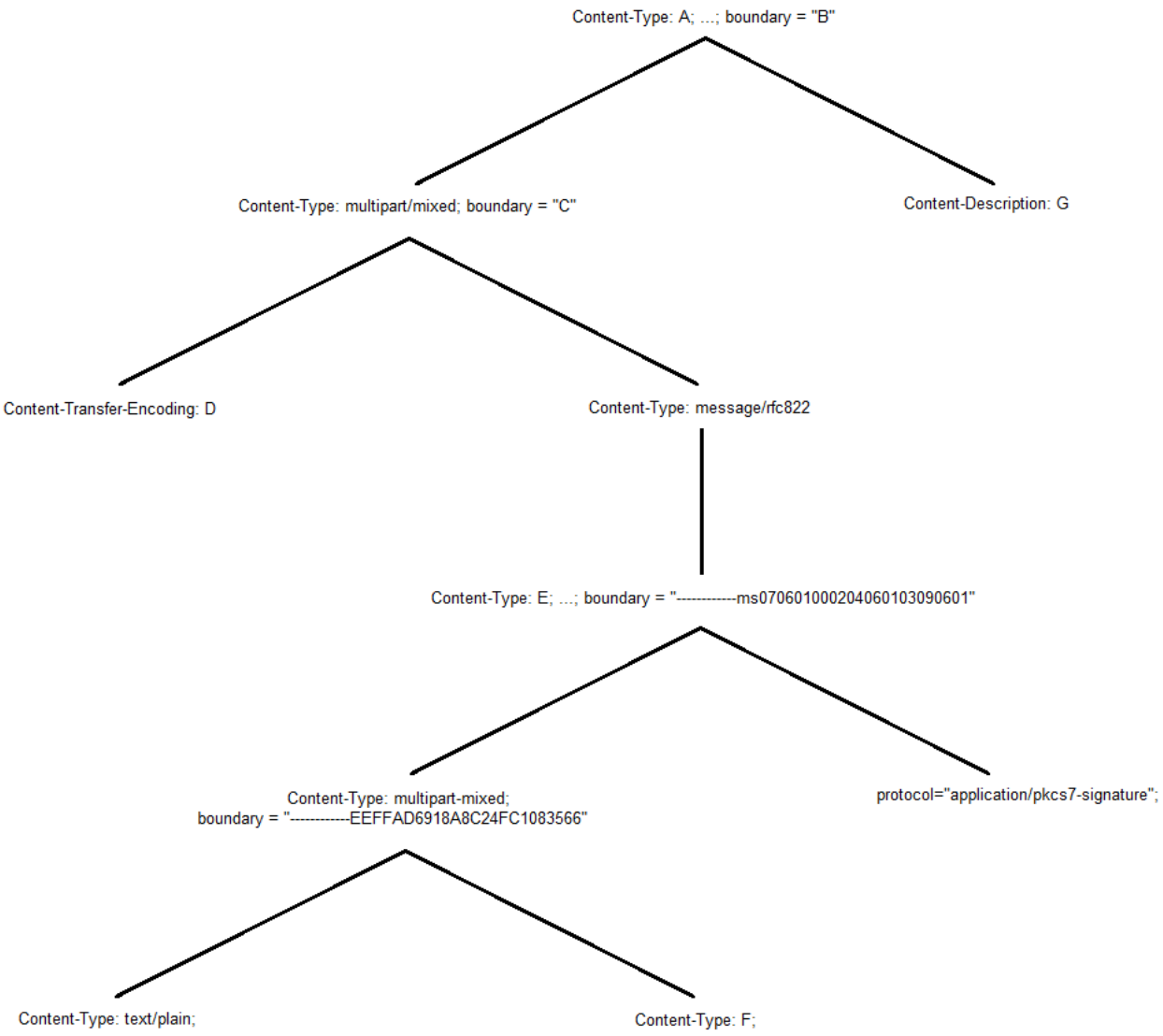
7️⃣

Exercise 7

Frage 1

Structure of MIME Bodies

Look at the file sourcetext.eml. The figure below shows schematically the structure of the MIME body of this file. Unfortunately, some information is missing. Specify them. Specify **only the contents of the *requested* fields.**



- A =

> Antwort:
> `multipart/signed`

- B =

> Antwort:
> `ms050406060406000802010907`

- C =

> Antwort:
> `30F62B2FE8BEAEAE8C866476`

- D =

> Antwort:
> `quoted-printable`

- E =

> Antwort:
> `multipart/signed`

- F =

> Antwort:
> `application/pdf`

- G =

> Antwort:
> `S/MIME Cryptographic Signature`

Frage 2

MIME certificate

The archive *bundle.zip* contains the following files:

· *ca.crt* - certificate file of the CA "Bruce

· *ca.key* - key pair to the CA

· *smime.cnf* - A configuration file for OpenSSL

· *generate.sh* - A script used to create the CA and certificate for Chuck Norris.

Note: The secret key is not password protected.

Use the given files to have the CA "Bruce Schneier" create a personal email certificate for you. Use the following parameters:

- Use an RSA key pair with 4096 bit modulus.
- Enter your name as Common Name (CN).
- Enter your email address as emailAddress.
- Set the extensions and use flags with OpenSSL as follows:
  - addtrust emailProtection
  - addreject clientAuth
  - addreject serverAuth
  - trustout
  - extfile smime.cnf
  - extensions smime

The certificates created in this way should be valid in many e-mail clients. We have tested this with a current version of Thunderbird. However, we cannot guarantee that all e-mail clients will accept the certificates created in this way, as they may have different requirements. You can use the commands in generate.sh as a guide. But be sure to use the CA provided for download!

Note that some email clients expect a certificate in PKCS12 format (see script).

Send a mail signed with your certificate to your tutor. As subject please use "[isits] Task 7 - Question 2 - S/MIME Mail" and as text please enter the names of all group participants. Only one mail has to be sent per group (you do not have to enter anything in the answer field).

> Antwort:

Frage 3

S/MIME signature

We consider the signed email file You_are_awesome.eml.

1. Over which lines of the message is the hash for the signature formed? The line Message-ID: ... is line 1

> First line that is hashed:
>
> `15`
>
> Last line that is hashed:
>
> `23`

2. Therefore, what are the boundaries that decide which part is signed?

> Boundary =
> `ms000301080506050507070207`

💡 For the subsequent changes to the source text of the e-mail, specify whether the respective change causes the signature verification on the recipient side to fail (CORRECT) or not (FALSE). The mail will not be re-signed after the change.

Note 1:
In each case, be clear about why verification (does not) fail.

Note 2:
You can also practically check the validity of the signature if your email client accepts the CA certificate ca.crt from the previous task and the certificate for Chuck Norris.
We have tested this with a recent version of Thunderbird (the modified .eml files can be dragged and dropped into a mailbox). However, we cannot guarantee that all email clients will accept the certificates created in this way, as there may be different requirements.

Note 3:

Score a signature as invalid (i.e. check CORRECT) if no signature is displayed at all
due to your changes (e.g. if the structure of the e-mail can no longer be processed).

Frage 4

Replace “ms000301080506050507070207"
with "BRUCE" in lines 14, 24, 84 in the boundary.

Bitte wählen Sie eine Antwort:

- [x] ~~Richtig~~
- [ ] Falsch

Frage 5

Make the changes from the previous question in line 10 as well.

Bitte wählen Sie eine Antwort:

- [ ] Richtig
- [x] ~~Falsch~~

Frage 6

Remove the header: X-Advertisement

Bitte wählen Sie eine Antwort:

- [ ] Richtig
- [x] ~~Falsch~~

Frage 7

Replace the *Display Name* in the From header - "Chuck Norris" - with your own name. Do not make any changes to the email address part in this line.

Bitte wählen Sie eine Antwort:

- [x] ~~Richtig~~
- [ ] Falsch

Frage 8

Add *Jonathan Katz (JK <jonathan@katz.org>)* as another addressee. Bruce Schneier should not notice that the mail has a second addressee.

Bitte wählen Sie eine Antwort:

- [ ] Richtig
- [x] ~~Falsch~~

Frage 9

In the text/plain part, change the text from "do the roundhousekick" to "run flash on a MAC".

> Bitte wählen Sie eine Antwort:
>
> - [x] ~~Richtig~~
> - [ ] Falsch

Frage 10

Replace the description of the signature encoding from base64 to quoted-printable.

> 💡 *Note: Assume that the mail client strictly adheres to the specified encoding.*

> Bitte wählen Sie eine Antwort:
>
> - [x] ~~Richtig~~
> - [ ] Falsch

Frage 11

Replace each occurrence of "awesome" with "super awesome" so that this can be read by the recipient without having to look in the source code.

> Bitte wählen Sie eine Antwort:
>
> - [ ] Richtig
> - [x] ~~Falsch~~