Exercise 8

Frage 1

What security goals do you want to achieve with email signatures?

> Wählen Sie die richtige(n) Antwort(en) aus:
>
> - [x] ~~Integrity~~
> - [x] ~~Authenticity~~
> - [ ] Anonymity
> - [ ] Confidentiality
> - [ ] Server-to-server security

Frage 2

Specify which line of the following email is signed.

Example answers: 3 or 3-4 or 3-4,13-14

```
 1. To: foo@example.com
 2. From: bar@example.com
 3. Subject: Remember This
 4. Date: Mon, 7 Jan 2019 17:22:40 +0100
 5.
 6. -----BEGIN PGP SIGNED MESSAGE-----
 7. Hash: SHA256
 8.
 9. Soylent Green
10. is PEOPLE!
11. -----BEGIN PGP SIGNATURE-----
12. Version: GnuPG v2
13.
```

```
iQIzBAEBCAAdFiEEPLDoRBatUvfhhlQYiLCNWle2IUAFAlwzhHkACgkQiLCNWle2
IUA6PQ//TKdpligpxVH54N6jClmAjqrgSa6zxWvxn9po89T5KRiJYw4+QY/AlABU
qr0W/FT9iGhdKcQ6BC01AWdfHI3jDNsdyuVuyHddPOzwL7W7X/6DjsubdrahvAnm
iLERCj7CCcYQhYux+xxswE0f8gsgAPiIScN5klmUZz1mZ7C3HA5EDH0v2V3CBytL
CchOo1L/I4pyeAioEXDxHhC/6G6OYi19JhGiRZmsSFAycY75ipv9QKNEIEyfTig8
QeN1jfkvtN2hXKZVrWzGkbuF5bVh3FTqq2ghfSULI/LF3E4/K/f1bWYhYjwMI/M6
HMCPpC4MICx9MM8b6j9Rez9Sc4NznYPF2mBRQegb/Ts1rwYQyIx8G9ruRwXuP3lq
3c9ozSe0fx3icc5K5FSE1HPz/gdazduCp2tzJ/55ze4Za6In6m7zZLkiXRepNA2j
uWz+pK6seF1I+7RowMr2rGSavrjUBu1pLGJ+9tMGU5t49D9DZSyThF534dOa9HlO
p3xVnJllDhFF2vnfSre2hoesR9tO4OANF/n0Qxaxh7sK/gsTtLvjkvGW7sNTtTGo
KxkifhGFBnnIUK1U2QVYaz4eAz9YG6c07z75xHLsgGLl3F0S+bAZG2GEIGqmoNRY
RfYqApzQYetSxYay68F/otI/hgN+xQt5LDRern3fZ6GBeY1tt/I=
=+C5n
-----END PGP SIGNATURE-----
```

> Antwort:
> `9-10`

Frage 3

Which statements are correct?

> Wählen Sie die richtige(n) Antwort(en) aus:
>
> - [x] ~~S/MIME uses a Certificate Authority (CA) to evaluate the validity of an email address.~~
> - [ ] S/MIME leaves it up to the user to evaluate the validity of an email address.
> - [ ] PGP uses a Certificate Authority (CA) to evaluate the validity of an email address.
> - [x] ~~PGP leaves it up to the user to evaluate the validity of an email address.~~

Frage 4

What are the reasonable requirements for email clients?

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

- [ ] It is always enough to display a signature status for all parts of an e-mail
- [x] ~~The security indicators must not be displayed within the e-mail body of an HTML e-mail.~~
- [ ] The security indicators are allowed to contradict each other as long as most of them are correct.
- [x] ~~It must be clear who created a signature.~~

Frage 5

Can signatures in the context of S/MIME help against these attacks?

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

- [ ] Yes, but only if encrypt-then-sign is used
- [ ] No
- [x] ~~Yes, but only if sign-then-encrypt is used~~

Frage 6

The Efail attacks on S/MIME generally have a greater impact than the attacks on OpenPGP. Why is this the case?

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

- [ ] OpenPGP uses CFB.

- [ ] OpenPGP libraries were written in secure programming languages.
- [x] ~~OpenPGP uses MDCs.~~

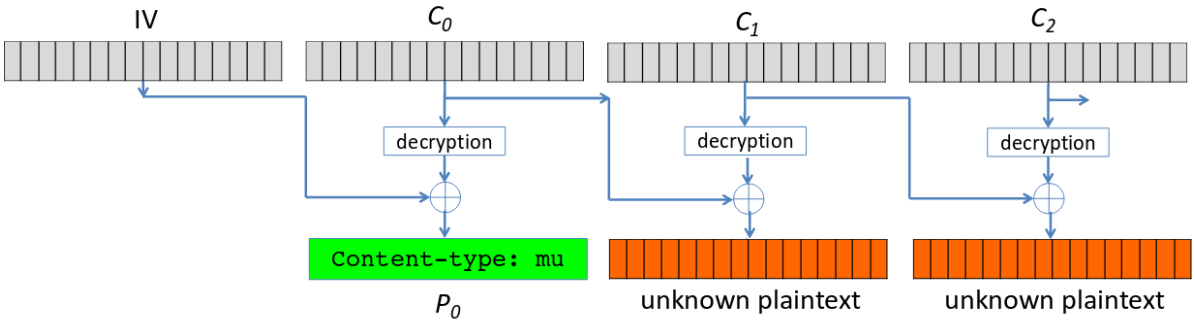
Frage 7

CBC Malleability

Given an S/MIME encrypted message with the following values:

IV: 70ccb336fed2ff10819a78aa36fd7c22

C_0: 4ca5de51dea18d73bcb557cf189e120d



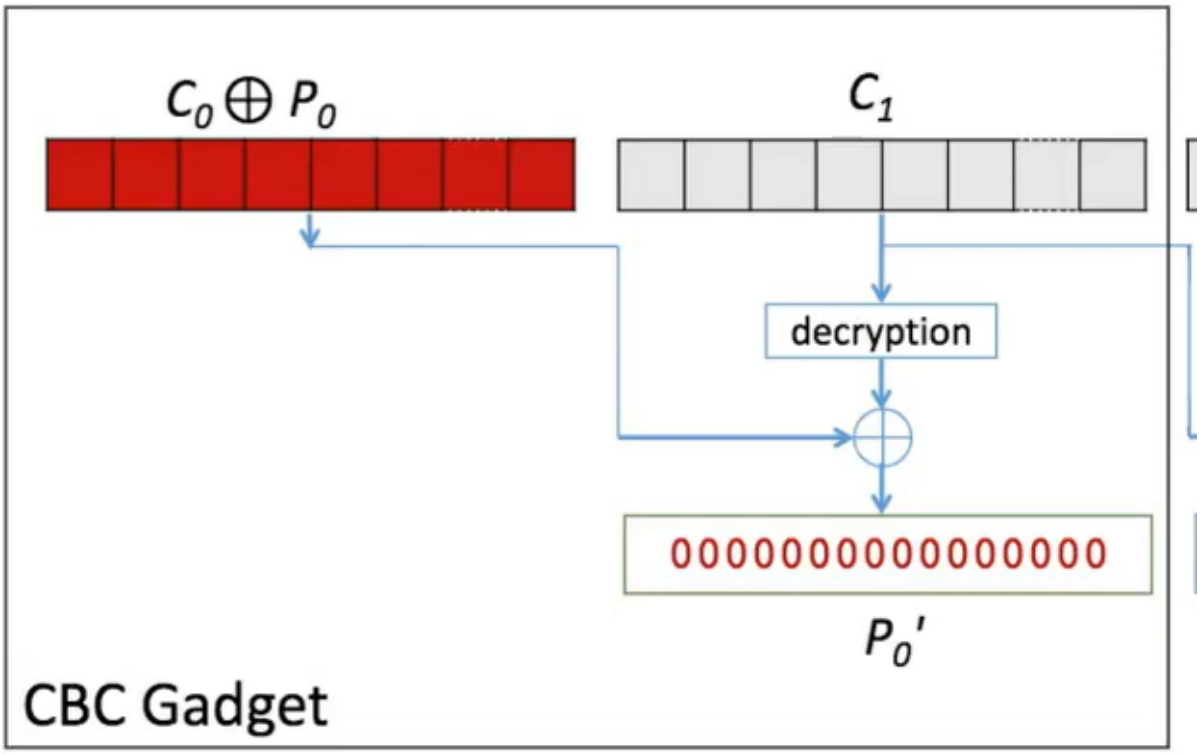
Modify the IV to produce `<img src=//e.cn/` in the plaintext block P_0 after decryption, which sends (interpreted as HTML) the plaintext from the subsequent blocks to the web server e.cn. What is the modified IV?

Solution (please enter hexadecimal without spaces and without 0x in front):

`payload = 0xfcab025bbcff95ec8cc27aa22be7f78`

Aus Video (*Timestamp: 26:00*) : https://www.youtube.com/watch?v=Tr6qhw7Vmus

Malleability of CBC



Malleability of CBC