QUIZ

Lecture 3

Question 1

- Suppose that **Alice** wishes to obtain a reliable public key for **Bob** for exchanging emails

- **Bob** could send his public key to **Alice** by email, and after that **Alice** could copy this key into her public-key keyring

- **Bob** could publish his public key on his personal website

- Are these good approaches?

Answer 1

- If **Eve** intercepts that email from **Bob**, she can send her own key to **Alice** instead.
- **Eve** may hack **Bob's** website and replace his key
- What **Bob** could actually do:
  - Give a key to **Alice** on a piece of paper
  - Send the key to **Alice**, and then confirm the correctness of the key fingerprint over the phone
  - Use a trusted third-party such as PGP or a trusted certificate

Question 2

- Let **sk(A)** be the secret key of **Alice**, and **pk(B)** be the public key of **Bob**

- **Alice** encrypts the message **m** with **sk(A)** and sends it to **Bob**

- What security properties are guaranteed for **Bob** when he receives **m**?

- What if **Alice** sent **m** encrypted with **pk(B)**?

Answer 2

- Authenticity: **anyone** can read the message, but it definitely came from **Alice**

- Confidentiality: only **Bob** can read the message, but it could come from **anyone**

Question 3

- **Alice** sends an encrypted and signed message to **Bob**

- When sending an encrypted and authenticated message with PGP, the signature could be applied before the encryption (or vide versa)

- Which method is preferable? Why?

Answer 3

- **Sign-then-encrypt**: **Bob** can decrypt, verify **Alice's** signature and confirm that the message indeed came from **Alice**

- **Encrypt-then-sign**: **Eve** can eavesdrop, capture **Alice's** message, replace the signature, and **Bob** will think that the message came from **Eve**

Question 4

- Why does PGP apply signature before applying compression?

Answer 4

- When signing the message before compression, the receiver only has to store the uncompressed message to verify the signature

- If the message was signed after compression, the receiver either has to store the compressed message, or apply compression before she can verify the signature