Answers to Exercise 1

1- A(n) …… function creates a message digest out of a message

- a) encryption
- b) decryption
- **c) hash**
- d) none of the mentioned

2- A digital signature needs a(n) …… system

- a) symmetric key
- **b) asymmetric key**
- c) either a) or b)
- d) neither a) nor b)

3- A difference between the PKI used by TLS for web browsers and the Web of Trust used by PGP is

- **a) PGP keys can be signed by any other user**
- b) PGP keys are certified in a hierarchical manner
- c) PGP keys have no expiry date
- d) PGP keys can use any type of public-key algorithms

4- Which of the following is true about Public-key Infrastructure?

- a) PKI uses two-way symmetric key encryption with digital certificates, and Certificate Authority.
- b) PKI uses private and public keys but does not use digital certificates.
- **c) PKI is a combination of digital certificates, public-key cryptography, and certificate authorities that provide enterprise wide security.**
- d) PKI uses only symmetric key encryption.

5- Digital signature provides

- a) authentication
- b) non-repudiation
- **c) both a) and b)**
- d) neither a) nor b)

6- PGP uses

- **a) a web of trust between the participants**
- b) a hierarchical trust model
- **c) public-key cryptography**
- **d) different levels of trust**

Answers to Exercise 2

1- First, Alice encodes the message, based on the position of each letter in the alphabet, such that

Letter	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Encoded Letter	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

The message "meet at noon" is encoded as follows

$$13,5,5,20,1,20,14,15,15,14$$

Second, for each encoded letter $c_i (i = 0, \dots, 9)$, Alice "decrypts" the message using her private key, i.e., she computes $s_i = m_i^{d_a} mod\ n_a = m_i^3\ mod\ 33$:

$13^3\ mod\ 33 = 19$

$5^3\ mod\ 33 = 26$

$20^3\ mod\ 33 = 14$

$14^3\ mod\ 33 = 5$

$1^3\ mod\ 33 = 1$

$15^3\ mod\ 33 = 9$

The signature is

$$19,26,26,14,1,14,5,9,9,5$$

Alice can now send the message and the signature to Bob.

2- Bob uses Alice's public-key to verify the signature. For each character $s_i (i = 0, \dots, 9)$ of the signature, Bob "encrypts" the signature with the public-key of Alice, i.e.., he computes $m'_i = s_i^{e_a} mod\ n_a = s_i^7\ mod\ 33$:

$$13,5,5,20,1,20,14,15,15,14$$

As the result is identical to the message, i.e., $\bigwedge_{i=0,\dots,9} m_i = m'_i$ is valid, the signature is correct.

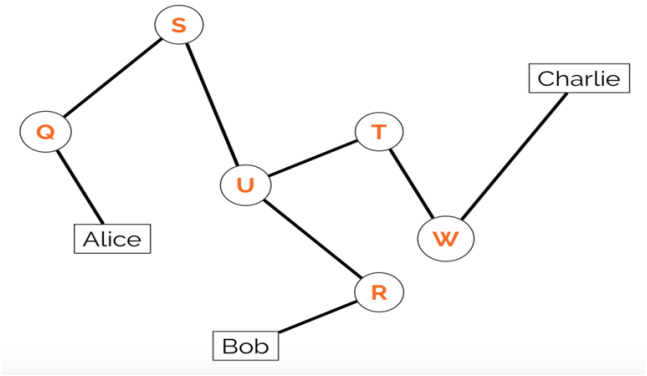
3- If Alice is using the same RSA key pair for signing documents and encrypting messages, Eve could trick Alice into signing a message that is encrypted with her public-key and, by that, trick Alice into decrypting this message for Eve.

$$c_i = m_i^{e_a} mod\ n_a$$

$$s_i = c_i^{d_a} mod\ n_a$$

Answers to Exercise 3

1- See the Figure below, the missing values are marked in **orange**



following certificates need to be stored by the different CAs:
Q: Alice
S: Q
U: S, T, R
R: Bob
T: W
W: Charlie
The users Alice, Bob, and Charlie only need to maintain their own public keys as well as the public-key (certificate) of the root CA (U). With this information, they can validate all certificates along the chains.

3- The following actions should be taken:
   a- Alice's CA (i.e., Q) needs to inform all its users (i.e., Alice) and the CA that issued its certificate (i.e., S).
   b- The CA that issued the certificate of Alice's CA (i.e., S) needs to publish the certificate of Alice's CA (i.e., Q) in its revocation list. The other CAs do not need to do an immediate action.
   c- When Charlie validates the public-key of Alice, Charlie needs to check the validity of all intermediate CAs. This includes checking the list of revoked certificates for each CA. Thus, Charlie should detect that the CA that signed the new (faked) certificate for Alice is no longer valid (is revoked).

Answers to Exercise 4

1. Reasons for intermediate CAs include:
   - *Performance:* The root CA can use stronger key pair as less certificates need to be signed.
   - *Security:*
     - The root CA certificate can be stored in a highly secure environment (e.g., offline) as only a few certificates need to be signed.
     - Reducing the risk associated with a compromised CA certificate (less users affected, i.e., a smaller number of certificates need to be revoked).
   - *Scalability:* Reducing the work load (signing request) for a CA. Intermediate CA can, e.g., be organized "by country/region" or along the organizational structure of an enterprise.

2. Initially, a user (e.g., Bob) only trusts the root CA. By checking the signatures along the certificate chain, this trust is transitively extended until, e.g., he can validate Alice's certificate. For this to work, Bob needs to trust all CA's along the chain to be honest, i.e., to only sign certificates after a thoroughly identity check (the certificate chain is only as strong as its weakest link).

Answers to Exercise 5

1. Self-signed certificates are allowing organizations or individuals to create “arbitrary” certificates without the need of a third party. In our scenario, the main reason might be that the bank can save the costs for getting a certificate signed by a third-party CA (and also creating self-signed certificates might be faster).

   Other common use cases are:
   - the generation of internal certificates for a closed user group (e.g., for web servers only accessible within a company’s intranet)
   - temporary certificates for testing purposes
   - until recently, properly-signed certificates where rather at expense. Thus, a lot of hobbyist websites used self-signed certificates to provide a confidential communication channel. This use case is discouraged with the availability of CA’s that issue certificates without costs, e.g., Let’s Encrypt (https://letsencrypt.org/).

2. Without further ways of validating a self-signed certificate, a web server with a self-signed certificate only provides an encrypted channel (i.e., secrecy) but no *authenticity*.

3. If customers need to visit a branch of the bank for opening an account, this would allow the bank to hand over the public-key of the self-signed certificate (or at least its fingerprint). This allows customers to import the certificate in their local certificate store (i.e., of their web browser), respectively, to check its authenticity using the securely and authentic transmitted fingerprint.

Answers to Exercise 6

Hint: To draw the graph, we first start drawing the different nodes (Alice, Bob, Carl, Dave, Fred, Garry, and Elena). Then, we draw –strong lines– for certification validation, starting by Alice's keyring table. For instance, we should verify sub-sections under Alice's keyring table and check which entities have certified their respective keys. If Alice has signed the key of an entity, (e.g., Bob), that is included in her keyring table, we can deduce Alice has certified the key of this entity (Bob).

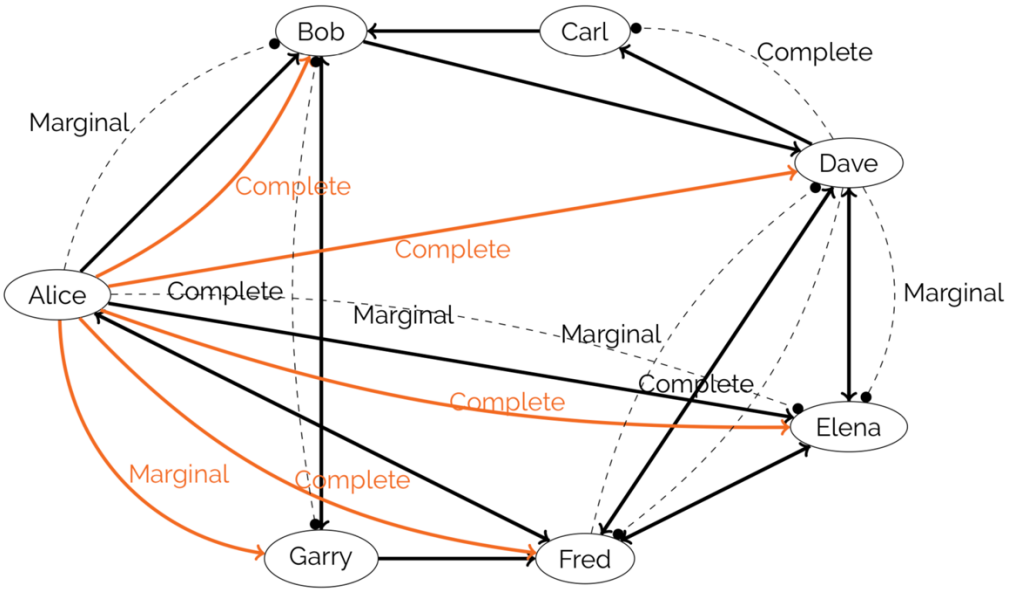


Table 1: Public Keyrings for Alice, Bob, Carl, Dave, Fred, Garry, and Elena