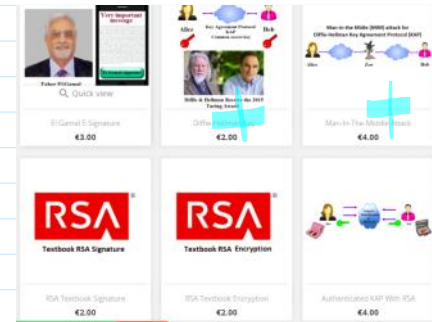


Koliokviumas : Lapkivcio 3d. 19:15.

<https://imimsociety.net/en/14-cryptography>

Sign in P. Vardas → 10 € kreditas

Get Reward



Cryptography: Information Confidentiality, Integrity, Authenticity and Authority (Person Identification).

Symmetric cryptography ----- Asymmetric cryptography 1976 Public Key CryptoSystems - PKCS

Symmetric encryption:

- block ciphers
- stream ciphers

H-functions, Message digest

HMAC H-Message Authentication Code

Asymmetric encryption

E-signature - Public Key Infrastructure - PKI

E-money

E-voting

Digital Rights Management - DRM: Marlin

Etc.

Public Key CryptoSystems - PKCS

1. Principles of Public Key Cryptography

Instead of using single symmetric key shared in advance by the parties for realization of symmetric cryptography, asymmetric cryptography uses two *mathematically* related keys named as private key and public key we denote by **PrK** and **PuK** respectively.

PrK is a secret key owned personally by every user of cryptosystem and must be kept secretly. Due to the great importance of **PrK** secrecy for information security we labeled it in red color. **PuK** is a non-secret personal key and it is known for every user of cryptosystem and therefore we labeled it by green color. The loss of **PrK** causes a dramatic consequences comparable with those as losing password or pin code. This means that cryptographic identity of the user is lost. Then, for example, if user has no copy of **PrK** he get no access to his bank account. Moreover his cryptocurrencies are lost forever. If **PrK** is got into the wrong hands, e.g. into adversary hands, then it reveals a way to impersonate the user. Since user's **PuK** is known for everybody then adversary knows his key pair

(PrK, PuK) and can forge his Digital Signature, decrypt messages, get access to the data available to the user (bank account or cryptocurrency account) and etc.

Let function relating key pair (PrK, PuK) be F . Then in most cases of our study (if not declared opposite) this relation is expressed in the following way:

$$\text{PuK} = F(\text{PrK}).$$

$$a = g^x \text{ mod } p$$

In open cryptography according to **Kerchoff principle** function F must be known to all users of cryptosystem while security is achieved by secrecy of cryptographic keys. To be more precise to compute PuK in function F must be defined using some parameters named as public parameters we denote by PP and color in blue that should be defined at the first step of cryptosystem creation. Since we will start from the cryptosystems based on discrete exponent function then these public parameters are

$$\text{PP} = (p, g).$$

Notice that relation represents very important cause and consequence relation we name as the direct relation: when given PrK we compute PuK.

Let us imagine that for given F we can find the inverse relation to compute PrK when PuK is given. Abstractly this relation can be represented by the inverse function F^{-1} . Then

$$\text{PrK} = F^{-1}(\text{PuK}).$$

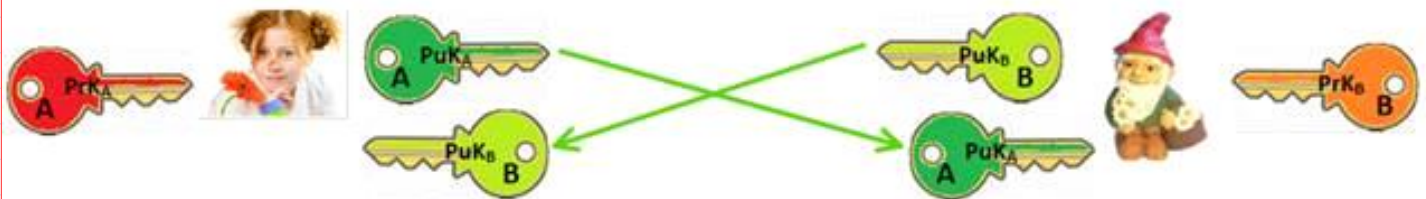
In this case the secrecy of PrK is lost with all negative consequences above. To avoid these undesirable consequences function F must be **one-way function** – OWF. In this case informally OWF is defined in the following way:

1. The computation of its direct value PuK when PrK and F in are given is effective.
2. The computation of its inverse value PrK when PuK and F are given is infeasible, meaning that to find F^{-1} is infeasible.

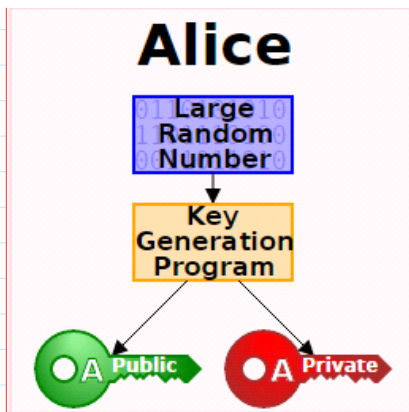
The one-wayness of F allow us to relate person with his/her PrK through the PuK. If F is 1-to-1, then the pair (PrK, PuK) is unique. So PrK could be reckoned as a unique secret parameter associated with certain person. This person can declare the possession or PrK by sharing his/her PuK as his public parameter related with PrK by and and at the same time not revealing PrK.

So, every user in asymmetric cryptography possesses key pair (PrK, PuK). Therefore, cryptosystems based on asymmetric cryptography are named as **Public Key CryptoSystems** (PKCS).

We will consider the same two traditional (canonical) actors in our study, namely Alice and Bob. Everybody is having the corresponding key pair (PrK_A, PuK_A) and (PrK_B, PuK_B) and are exchanging with their public keys using open communication channel as indicated in figure below.



Asymmetric Key Pair Generation



PrK and **PuK** are mathematically related by One-Way Function:

$$\text{PuK} = F(\text{PrK})$$

F is one-way function - OWF if:

1. For given F defined by public parameters and **PrK** it is easy to compute **PuK**.
2. For given F and **PuK** it is infeasible to find $\text{PrK} = F^{-1}(\text{PuK})$.

Public Parameters PP = (p, g): for F definition

$$\text{PrK} = x \leftarrow \text{randi} \implies \text{PuK} = a = g^x \text{ mod } p$$

2. Private Keys **Prk** and public Public Keys **PuK** generation.



$$\text{PrK}_A = x = \text{randi}(p-1)$$

$$a = g^x \text{ mod } p$$

$$\text{PuK}_A = a = \text{mod_exp}(g, x, p)$$

$$\text{PrK}_B = y = \text{randi}(p-1)$$

$$b = g^y \text{ mod } p$$

$$\text{PuK}_B = b = \text{mod_exp}(g, y, p)$$

1. Identification.

If person can prove that he/she knows **PrK** corresponding to his/her **PuK** without revealing any information about **PrK** then everybody can trust that he is communicating with person possessing (**PrK**, **PuK**) key pair. This kind of proof is named as **Zero Knowledge Proof** (ZKP) and plays a very important role in cryptography. It is very useful to realize identification, Digital Signatures and many other cryptographically secure protocols in internet. In many cryptographic protocols, especially in identification protocols **PrK** is named as **witness** and **PuK** as a **statement** for **PrK**.

Every actor is having the corresponding key pair (**PrK_A**, **PuK_A**) and (**PrK_B**, **PuK_B**) and are exchanging with their public keys using open communication channel as indicated in figure below. Let Bob is sure that **PuK_A** is of Alice and wants to tell Alice that he intends to send her his photo with chamomile flowers dedicated for Alice. But he wants to be sure that he is communicating only with Alice itself and with nobody else. He hopes that at first Alice will prove him that she knows her secret **PrK_A** using ZKP protocol. In general, this protocol is named as identification protocol, is interactive and has 3 communications to exchange the following data named as **commitment**, **challenge** and **response**.

Registration phase: Bank generates **PrK_A = x** and **PuK_A = a** to Alice and hands over this data

in smart card, or other crypto chip in Alice's smart phone, or in software for Smart ID.

Schnorr Id Scenario: **Alice** wants to prove **Bank** that she knows her **Private Key - PrK_A** which corresponds to her **Public Key - PuK_A** not revealing **PrK_A**: Zero Knowledge Proof - ZKP Protocol execution between **Alice** and **Bank** has time limit.

Alice's computation resources has a limit --> protocol must be computationally effective.

PrK_A=x is called a **witness** and corresponding **PuK_A=a=g^x mod p** is called a **statement**.

This protocol is initiated by Alice and has the following three communications.

P(x, a) - Prover - **Alice**

V(a) - Verifier - **Bank**

Public Parameters PP = (p, g)

- Alice** generates at random secret random number $u = \text{randi}(p-2)$ and using $PP=(p, g)$ computes **commitment t** in the following way

$$t = g^u \text{ mod } p, t \in \mathbb{Z}_{p-1} = \{0, 1, 2, \dots, p-2\}$$

Alice sends **t** and **a** to **Bank**.

- Bank** generates at random **challenge h** = $\text{randi}(p-2)$ and sends **h** to **Alice**.

- Alice** after receiving **h** computes her **response res** having her private key **x** together with previously generated secret number **u**:

$$res = u + xh \text{ mod } p-1; res \in \mathbb{Z}_{p-1} = \{0, 1, 2, 3, \dots, p-2\}$$

Alice sends **r** to the **Bank**.

After the third communication **Bank** verifies if the following identity holds:

$$g^{res} = t a^h \text{ mod } p.$$

P(x, a) - Prover - **Alice**

V(a) - Verifier - **Bank**

$$x \leftarrow \text{randi}(\mathbb{Z}_{p-1}); a = g^x \text{ mod } p$$

$$A: u \leftarrow \text{randi}(\mathbb{Z}_{p-1})$$

$$t = g^u \text{ mod } p$$

$$res = u + x \cdot h \text{ mod } (p-1)$$

$$B: a$$

$$h \leftarrow \text{rand}(\mathbb{Z}_{p-1})$$

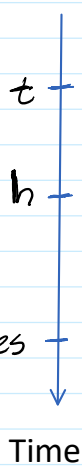
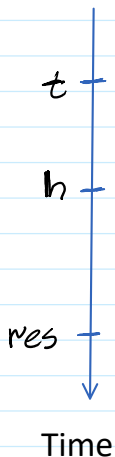
$$\text{Verifies if } g^{res} = t a^h \text{ mod } p$$

$$g^{res} = g^{(u+xh) \text{ mod } (p-1)} \text{ mod } p = g^u \cdot g^{xh} \text{ mod } p =$$

$$= t \cdot a^h \text{ mod } p.$$

<https://imimsociety.net/en/>

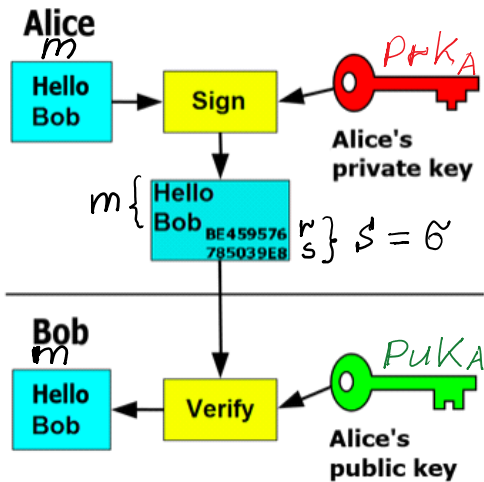
<https://imimsociety.net/en/14-cryptography>



Asymmetric Signing - Verification

$$S = \text{Sign}(\text{PrK}_A, m)$$

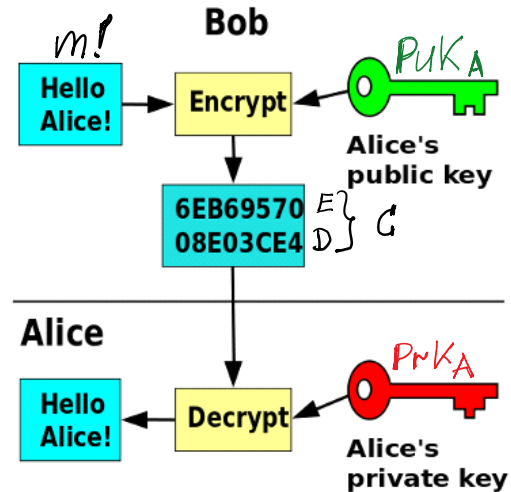
$$V = \text{Ver}(\text{PuK}_A, S, m), V \in \{\text{True}, \text{False}\} \equiv \{1, 0\}$$



Asymmetric Encryption - Decryption

$$c = \text{Enc}(\text{PuK}_A, m)$$

$$m = \text{Dec}(\text{PrK}_A, c)$$



In general, to create a signature on the message of any length M parties are using cryptographic secure H-function (message digest).

In Octave we use H-function

```
>> hd28('...') % the input '...' of this function represents a string of symbols between the commas.
                % the output of this function is decimal number having at most 28 bits.
```

Schnorr Signature Scheme (S-Sig).

Let M be a message in string format to be signed by Alice and sent to Bank: $\gg M = \text{'Hello Bob'}$

For signature creation Alice uses public parameters $PP = (p, g)$ and

Alice's key pair is $\text{PrK}_A = x, \text{PuK}_A = a$.

Alice chooses at random $u, 1 < u < p-1$ and computes first component r of his signature:

$$r = g^u \bmod p. \tag{2.19}$$

Alice computes H-function value h and second component s of his signature:

$$h = H(M || r), \tag{2.20}$$

$$s = u + xh \bmod p-1. \tag{2.21}$$

Alice's signature on h is $\sigma = (r, s)$. Then Alice sends M and σ to Bank.

After receiving M and σ , Bank according to (2.20) computes h' and verifies if

$$g^s \bmod p = r a^{h'} \bmod p. \tag{2.22}$$

Symbolically this verification function we denote by

$$\text{Ver}(a, \sigma, h) = V \in \{\text{True}, \text{False}\} \equiv \{1, 0\}. \tag{2.23}$$

This function yields True if (2.22) is valid $\leftarrow h = h'$ and $\text{PuK}_A = F(\text{PrK}_A)$.

```
>> m='Hello Bob'
```

```

m = Hello Bob
>> r=1234567
r = 1234567
>> cc=concat(m,r)
cc = Hello Bob1234567 % cc is a string type variable
>> cc=concat(m,'1234567')
cc = Hello Bob1234567
> h=hd28(cc)
h = 242519187
>> h=hd28('Hello Bob1234567')
h = 242519187

```

$$g^s = g^{(t+xh) \bmod (p-1)} \bmod p = g^t \cdot g^{xh} \bmod p = r \cdot (g^x)^{h'} \bmod p = r \cdot a^{h'} \bmod p.$$

If $h' = h$ & $a = g^x \bmod p \Rightarrow$ equation (2.22) is valid \Rightarrow
 \Rightarrow signature is formed with $PrK = x$ corresponding to
 $PuK = a = g^x \bmod p.$

AKAP

$A: PrK = x; PuK = a.$

$PuK_B = b; PuK_{TTP}.$

$u \leftarrow \text{randi}(\mathbb{Z}_{p-1})$

$t_A = g^u \bmod p$

$t \leftarrow \text{randi}(\mathbb{Z}_{p-1})$

$r = g^t \bmod p$

$h = H(t_A || r)$

$s = t + xh \bmod (p-1)$ $\xrightarrow{t_A, \sigma = (r, s)}$ $B: PrK_B = y; PuK_B = b.$
 $a = PuK_A$
 $Ver(a, \sigma, t_A) = True$

Till this place

① A browser verifies
TTP signature on

$\leftarrow t_B, \sigma_B = (r, s)$
 $Cert_B$ $\left(\begin{array}{l} V \leftarrow \text{randi}(\mathbb{Z}_{p-1}) \\ t - a^V \bmod p \end{array} \right.$

TTP signature on $\leftarrow^{u_B, v_B = (n, \gamma)}$
 Cert_B
 PuK_B .

② A verifies B signature

$\tilde{\sigma}_B = (R, s')$ on t_B

③ A computes common
secret key

$$k_{AB} = (t_B)^u \text{ mod } P$$

$$k_{AB} = k = k_{BA}$$

$$V \leftarrow \text{randi}(Z_{p-1})$$

$$t_B = g^V \text{ mod } P$$

$$l \leftarrow \text{randi}(Z_{p-1})$$

$$R = g^l \text{ mod } P$$

$$H = H(t_B || R)$$

$$s' = l + yH \text{ mod } (p-1)$$

$$\text{Cert}(\text{PuK}_B) = \text{Cert}_B$$

↑ signed

Trusted Third Party - TTP

$(\text{PrK}_{TTP}, \text{PuK}_{TTP})$

Veri sign

$$k_{BA} = (t_A)^v \text{ mod } P$$