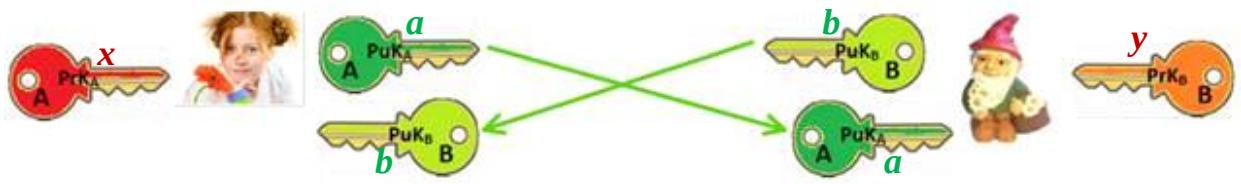
Cryptography: Information confidentiality, integrity, authenticity, person identification.

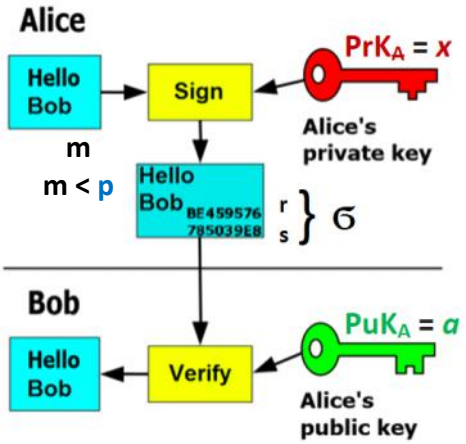


Message m < p

Asymmetric Signing - Verification

Sign(PrK$_A$, m) = σ = (r, s)

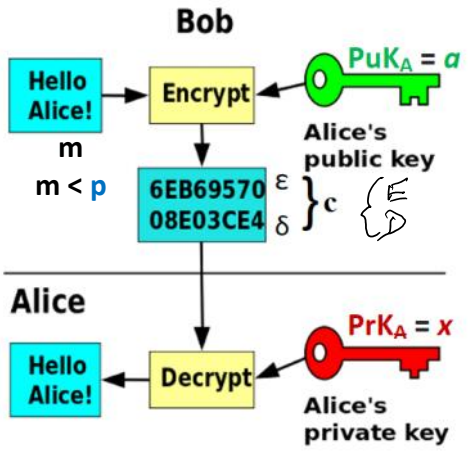
V=Ver(PuK$_A$, m, σ), V∈{True, False} ≡ {1, 0}



Asymmetric Encryption - Decryption

c=Enc(PuK$_A$, m)

m=Dec(PrK$_A$, c)



RSA Cryptosystem:

Euler totient function **ϕ(*n*)**: defines number of numbers **z** less than **n** that gcd(***z***,***n***)=1.

ϕ(*n*) = ϕ ≡ fy.

If ***n***=***p*******q*** where ***p***,***q***-primes then **φ(*n*) = ϕ = (*p*-1)*(*q*-1) ≡ fy**.

Let ***n***=3*5=15 --> **ϕ(*n*) = ϕ** = (3-1)*(5-1) = 2*4 = 8 ≡ **fy**.

$\mathcal{I}'_{15} = \{1, 2, 3, \ldots, 14\}$ * mod 15 ; $\mathcal{I}'_n = \{1, 2, 3, \ldots, n-1\}$ * mod n

>> gcd(1,15) = 1
>> gcd(2,15) = 1
>> gcd(3,15) = ?

Euler theorem. If gcd(***z***,***n***)=1 then

$$z^{\phi} = 1 \bmod n$$

$i \cdot j \bmod n = a^{i+j} \bmod n = a^{(i+j) \bmod \phi} \bmod n$

$z - 1 \bmod n$

$a^i a^j \bmod n = a^{i+j} \bmod n = a^{(i+j) \bmod \phi} \bmod n$

$(a^i)^j \bmod n = a^{i \cdot j} \bmod n = a^{(i \cdot j) \bmod \phi} \bmod n.$

According to Euler theorem exponents are computed mod ϕ.

Multiplication Tab. **Z15**															
*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	14	13	12	11	10	9	8	7	6	5	4	3	2	1

16 | 15
15 | 1
1

Exp. Tab. **Z15**															
^	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4
3	1	3	9	12	6	3	9	12	6	3	9	12	6	3	9
4	1	4	1	4	1	4	1	4	1	4	1	4	1	4	1
5	1	5	10	5	10	5	10	5	10	5	10	5	10	5	10
6	1	6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4
8	1	8	4	2	1	8	4	2	1	8	4	2	1	8	4
9	1	9	6	9	6	9	6	9	6	9	6	9	6	9	6
10	1	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1
12	1	12	9	3	6	12	9	3	6	12	9	3	6	12	9
13	1	13	4	7	1	13	4	7	1	13	4	7	1	13	4
14	1	14	1	14	1	14	1	14	1	14	1	14	1	14	1

$2^8 = 256 \bmod 15 =$
$= (255+1) \bmod 15 =$
$= \underbrace{255 \bmod 15}_{0} + 1 \bmod 15 = 1$

$\gcd(2,15) = 1 \rightarrow 2^8 = 1 \bmod 15$
$\gcd(3,15) = 3 \neq 1 \rightarrow 3^8 \neq 1 \bmod 15$
$\gcd(4,15) = 1 \rightarrow 4^8 = 1 \bmod 15$

$\gcd(z,n)=1$

$\mathcal{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$

$|\mathcal{Z}_{15}^*| = 8 = \phi(15) = \phi(3*5)$
$= (3-1)*(4-1)$

RSA key generation: 2048 bits arithmetics; we will use 28 bits arithm.

1. Two primes p, q are generated at random. $|q| = 1024$ bits $|p| = 1024$ bits
2. RSA module $n = p \cdot q$ is computed & $\phi(n) = (p-1)\cdot(q-1) = \phi$.
3. Random RSA exponent e: $\gcd(e, \phi) = 1$ is computed.
   According to RSA standard $e = 2^{16}+1$.
4. The inverse element to e mod ϕ is computed:
   $d = e^{-1} \bmod \phi \Rightarrow d\,e \bmod \phi = 1$.
5. $PrK = d$; $PuK = (n, e)$.

We use $|n| = 28$ bits $\rightarrow$ $|p| = |q| = 14$ bits

```
>> e=2^16+1
e = 65537
>> isprime(e)
ans = 1
```

Key Generation

```
>> p=genprime(14)
p = 11491
>> q=genprime(14)
q = 14087
>> n=p*q
n = 161873717
>> e=2^16+1
e = 65537
>> fy=(p-1)*(q-1)
fy = 161848140
>> d=mulinv(e,fy)
d = 34529513
>> mod(e*d,fy)
ans = 1
```

RSA textbook encryption

m - message: $m < n \sim 2^{2048}$; $|m| < 2048$ bits

$m \bmod n = m$

B: $\xleftarrow{PuK_A}$ A: $PuK_A = (n, e)$; $PrK_A = d$.

$c = Enc(PuK_A, m) = m^e \bmod n$ $\xrightarrow{c}$ $Dec(PrK_A, c) = m =$

$= c^d \bmod n =$

$= (m^e)^d = m^{ed} =$

$= m^{ed \bmod \phi} \bmod n =$ ($ed \bmod \phi = 1$)

$= m^1 \bmod n = m \bmod n = m$

```
>> m=int64(111222333)
m = 111222333
>> c=mod_exp(m,e,n)
c = 51722206
```

```
>> mm=mod_exp(c,d,n)
mm = 111222333
```

RSA textbook encryption is not randomised – is not probabilistic.

RSA textbook signature

RSA textbook signature

A : $PuK_A = (n, e)$; $PrK_A = d$.

m - message : $m < n \Rightarrow m \bmod n = m$

$\sigma = sign(PrK_A, m) = m^d \bmod n$ $\xrightarrow{m, \sigma}$ B: $PuK_A = (n, e)$

$Ver(PuK_A, \sigma, m) = \begin{cases} True \equiv 1 \\ False \equiv 0 \end{cases}$

>> sigma=mod_exp(m,d,n)
sigma = 149550780

$\sigma^e \bmod n =$

$= (m^d)^e \bmod n =$

$= m^{de \bmod \phi} \bmod n =$

$= m^1 \bmod n = m'$.

>> ver=mod_exp(sigma,e,n)
ver = 111222333

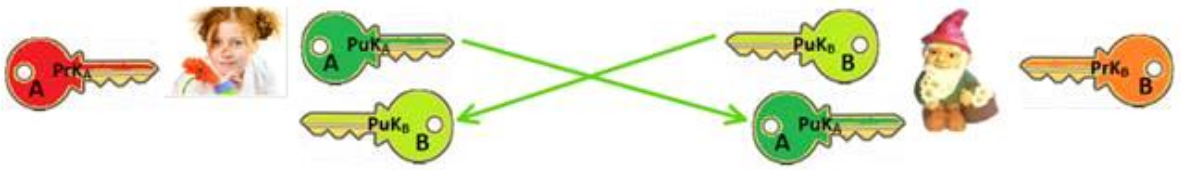
RSA textbook signature is a signature with message recovery.

If $m' = m$, then signature σ is formed by d corresponding to $PuK_A = (n, e) \Rightarrow True$

RSA AKAP

$PrK_A = d_A$; $PuK_A = (n_A, e_A)$.

$PrK_B = d_B$; $PuK_B = (n_B, e_B)$.



AKAP using RSA signature

$PuK_A = (n_B, e)$; $PrK_A = d_A$.

PuK_B

$PuK_B = (n_B, e)$; $PrK_B = d_B$.

PuK_A

$k_{AB} = (t_B)^u \bmod p =$

$= (g^v)^u \bmod p = g^{vu} \bmod p$

$k_{BA} = (t_A)^v \bmod p =$

$= (g^u)^v \bmod = g^{uv} \bmod p$

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

1) $Sign(d_A, t_A) = \sigma_A$

$\sigma_A = (t_A)^{d_A} \bmod n$

2) $Ver(PuK_B, \sigma_B, t_B) \in \{1, 0\}$

$t_B' = (\sigma_B)^{e_B} \bmod n_B = t_B$

3) $k_{AB} = (t_B)^u \bmod p$

1) $Ver(PuK_A, \sigma_A, t_A) \in \{1, 0\}$

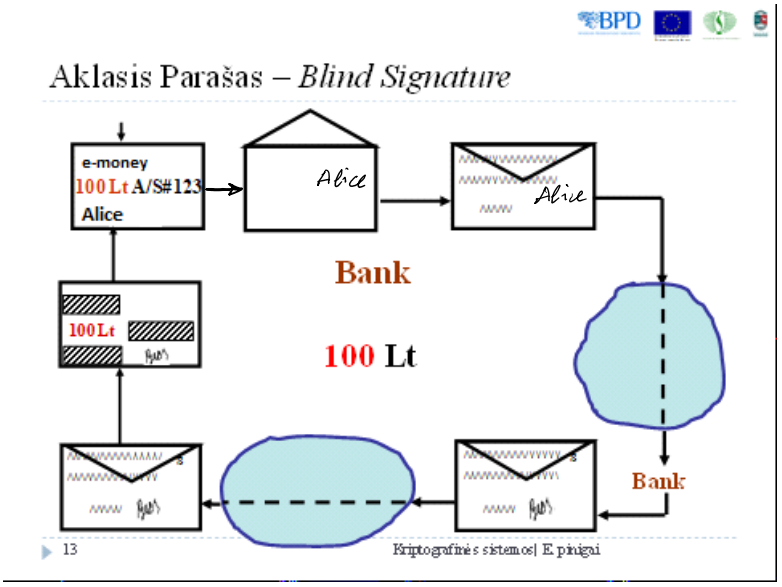
$t_A' = (\sigma_A)^{e_A} \bmod n_A = (t_A)^{d_A e_A} \bmod n$

$= t_A^1 \bmod n_B = t_A$

2) $Sign(d_B, t_B) = \sigma_B$

3) $k_{BA} = (t_A)^v \bmod p$

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



Chaum e-money system

e-coin

```
>> e=2^16+1
e = 65537
>> isprime(e)
ans = 1
```

RSA cryptosystem

B: $p, q \leftarrow genprime$

$n = p \cdot q$

$\phi = (p-1)\cdot(q-1)$

$e = 2^{16}+1$

$d = e^{-1} \bmod \phi$ $\Rightarrow$ $ed = 1 \bmod \phi$

$PuK = (n, e)$

$PrK = d$

```
>> d = mulinv(e, fy)   % fy = ϕ
```

If $e = 2^{16}+1$ – it is prime

1) $1 < e < \phi$

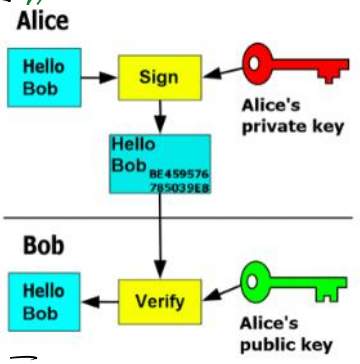
2) $gcd(e, \phi) = 1$ since e is prime

Since numbers e and d are presented in exponent, then exponent value is computed mod ϕ according to Euler theorem:

If $gcd(z, n) = 1 \Rightarrow z^{\phi} \bmod n = 1$

Any computations performed in the exponent are computed mod ϕ:

$$z^{e \cdot d} \bmod n = z^{e \cdot d \bmod \phi} \bmod n = z^1 \bmod n = z \quad \text{if } z < n$$



RSA signature creation:

On message M encoded by decimal number $m < n$.

$\text{Sign}(PrK = d, m) = \sigma = m^d \bmod n$.

RSA signature verification:

$\text{Ver}(PuK = (e, n), \sigma) = \sigma^e \bmod n = m$.

Correctness: $\sigma^e \bmod n = (m^d)^e \bmod n = m^{de \bmod \phi} \bmod n = 1 =$

$= m \bmod n \underset{\text{if } m < n}{=\!=} m$

A: $PrK_A = d_A$, $PuK_A = (n_A, e)$ $\quad \xleftarrow{PuK = (n, e)} \quad$ B: $Prk = d$, $PuK = (n, e)$.

Masking

A: $m = 100$; is masking value m:

$t \leftarrow$ randi; $1 < t < n$: $\gcd(t, n) = 1 \Rightarrow \exists!\ t^{-1} \bmod n$.

$m' = m \cdot t^e \bmod n$ $\xrightarrow{m'}$ B:

$\text{Ver}(PuK = (n, e), \sigma', m') = m'$ $\xleftarrow{\sigma'}$

$\text{Sign}(PrK = d, m') = \sigma'$

$\sigma' = (m')^d \bmod n =$

$= (m \cdot t^e)^d \bmod n =$

$= m^d \cdot t^{ed \bmod \phi} \bmod n = 1 =$

$= m^d \cdot t \bmod n$

$\sigma' = m^d \cdot t \bmod n$ $\xleftarrow{}$

UnMasking

A: unmasks signed m'

$(\sigma')^e \bmod n = ((m')^d)^e \bmod n = (m')^{ed \bmod \phi} \bmod n = 1 =$

$= m' \underset{\text{if } m' < n}{\bmod n =} m' \Rightarrow$ Signature is valid. = True

A: wants to find a valid signature σ of B on $m = 100$:

$\sigma = m^d \bmod n$

A extracts (unmasks) $m^d \bmod n = \sigma$ from σ':

A extracts (unmasks) $m^d \bmod n = \sigma$ from σ' :

$\sigma' \cdot t^{-1} \bmod n \rightarrow$ if $\gcd(t, n) = 1 \Rightarrow \exists!\ t^{-1} \bmod n$ exists.

$\sigma' \cdot t^{-1} \bmod n = m^d \cdot t \cdot t^{-1} \bmod n = m^d \bmod n = \sigma$.

But $m^d \bmod n$ – is a B's signature on the actual amount of money $m = 100$.

$\sigma = m^d \bmod n$.

$PuK = (n, e)$ B's

A : (m, σ) $\xrightarrow[\text{to the Vendor } V]{(m, \sigma)}$ V: verifies is B's signature on the money amount $m = 100$ is true

$Ver(PuK=(n,e), \sigma, m) = True$

$\sigma^e \bmod n = (m^d)^e \bmod n = m^{de \bmod \phi} \bmod n = m \bmod n = m$ if $m < n$

E-coin properties.

1. **Anonimity**.
2. **Untraceability**.
3. **Double-spending prevention**.
4. **Divisibility**.

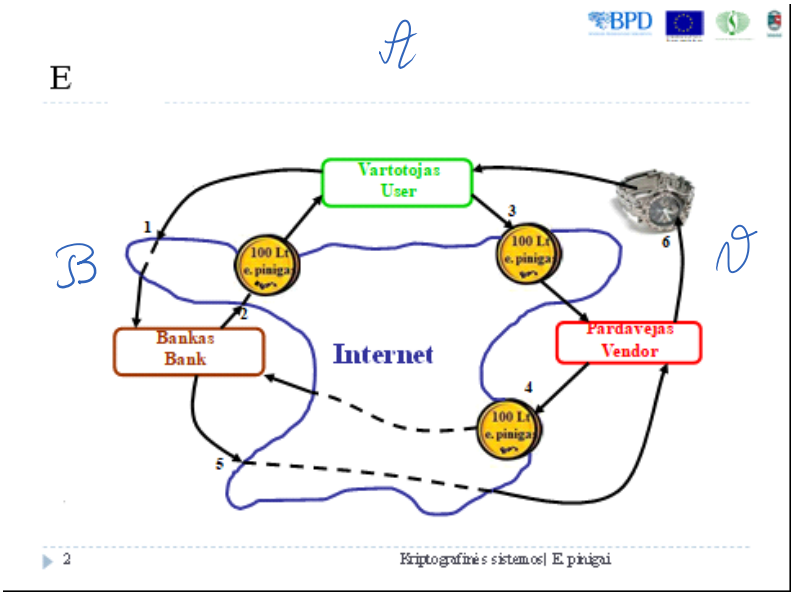
Chaum

Divisible coins (e-money) are growing is size.

A : $\xrightarrow{(m, \sigma), AD_1}$ V_1 $\xrightarrow{(m, \sigma), AD_1, AD_2}$ V_2 ——————

$\xrightarrow{(m, \sigma), AD_1, AD_2, AD_3}$ V_3 – – – – – –

growing in size



e-money anonimity

Cut and Choose

Till this place