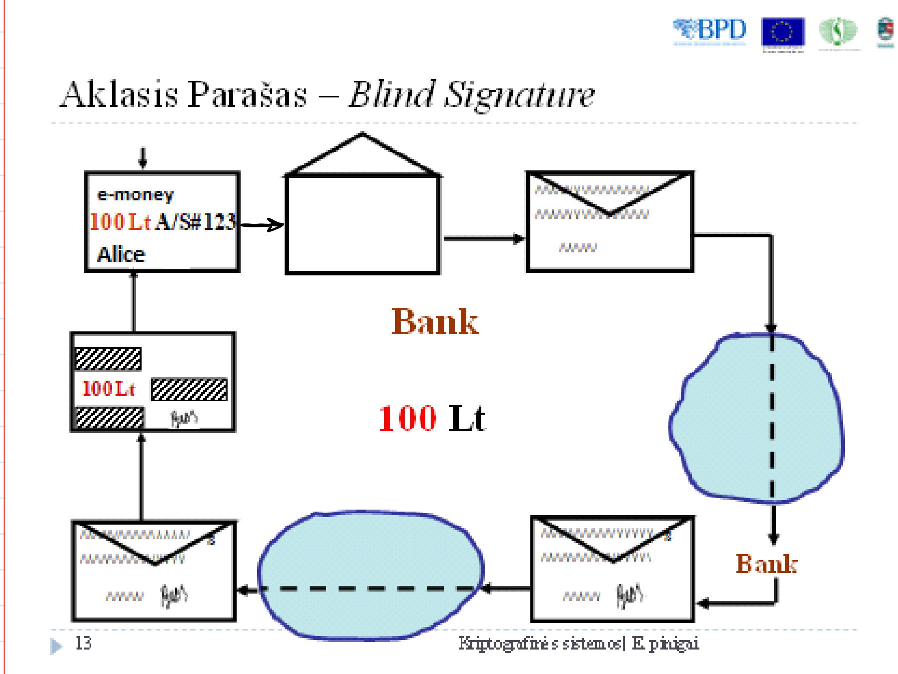
Finally the defendance of Course Works (CW) according to our curricular will be held on:
December 19 at 15:30 in 103f and on
December 21 at 13:30 in 238 class.
CW list is presented in my Google drive

https://docs.google.com/document/d/1GDVZuRPtmQ5Z--IdqGunPx_3qOGSfrpR/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

Please choose topic and label it by the first letter of surname dot name, e.g. S.Name.
For some of topics the group project realization can take place after you inform me by e-mail (below) or during the lecture.
Requirements for CW you can find in
http://crypto.fmf.ktu.lt/xdownload/
in files Course_Work
It is preferable to prepare slides, text and oral report in English.
Zipped CW you should send to my e-mail before the presentation
eligijus.sakalauskas@ktu.lt

Exam will be held in January 16, from 14:00-16:00, in class 506.



Chaum e-money system
e-coin

RSA cryptosystem

B: $p, q \leftarrow$ genprime

$n = p \cdot q$

$\phi = (p-1)\cdot(q-1)$ $\quad$ $PuK = (n, e)$

$e = 2^{16}+1$ $\quad$ $ed = 1 \mod \phi$

If $e = 2^{16}+1$ – it is prime

1) $1 < e < \phi$

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

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

$$\left.\begin{array}{l} e = 2^{16}+1 \\ d = e^{-1} \bmod \phi \end{array}\right\} \Rightarrow \begin{array}{l} e\,d = 1 \bmod \phi \\ PrK = d \end{array}$$

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

`>> d = mulinv(e, fy)   % fy = φ`

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:

$$z^{e\cdot d} \bmod n = z^{e\cdot d \bmod \phi} \bmod n = z^1 \bmod n = z$$

if $z < n$

A: $PrK_A = d_A$, $PuK_A = (n_A, e)$ $\quad\quad$ $PuK = (n, e)$ $\quad\quad$ B: $PrK = d$, $PuK = (n, e)$.

A: $m = 100$

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

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

$\mathrm{Ver}(PuK = (n, e), \sigma', m') = T \xleftarrow{\sigma'}$ $\quad\quad$ $\mathrm{Sign}(PrK = d, m') = \sigma'$

$$\sigma' = (m')^d \bmod n =$$
$$= (m \cdot t^e)^d \bmod n =$$
$$= m^d \cdot t^{ed \bmod \phi} \bmod n =$$
$$= m^d \cdot t \bmod n$$

$$(\sigma')^e \bmod n = ((m')^d)^e \bmod n = (m')^{\overbrace{ed \bmod \phi}^{=1}} \bmod n =$$
$$= m' \bmod n = m' \Rightarrow \text{signature is valid.} = T.$$

if $m' < n$

$\mathcal{A}$: wants to find a valid signature $\mathcal{B}$ σ on $m=100$:
$\sigma = m^d \bmod n$

$\mathcal{A}$ extracts (unmasks) $m^d \bmod n$ from σ' :
$\sigma' \cdot t^{-1} \bmod n \longrightarrow$ if $\gcd(t, n) = 1 \Rightarrow t^{-1} \bmod n$ exists.
$\sigma' \cdot t^{-1} \bmod n = \underbrace{m^d \cdot \cancel{t}} \cdot \underbrace{\cancel{t^{-1}}} \bmod n = \underbrace{m^d \bmod n = \sigma.}$

But $m^d \bmod n$ - is a $\mathcal{B}$'s signature on the actual amount of money $m = 100$.
$\sigma = m^d \bmod n$.

$PuK=(n, e)$ $\mathcal{B}$'s

$\mathcal{A}$: (m, σ) $\xrightarrow[\text{to the Vendor } \mathcal{V}]{(m,\sigma)}$ $\mathcal{V}$: verifies is $\mathcal{B}$'s signature on the money amount $m = 100$ is true
$Ver(PuK=(n,e), \sigma, m) = T$

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

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

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

$\mathcal{A}$: $\xrightarrow{(m,\sigma), AD_1}$ $\mathcal{V}_1$ $\xrightarrow{(m,\sigma), AD_1, AD_2}$ $\mathcal{V}_2$ ——————
$\xrightarrow{(m,\sigma), \underbrace{AD_1, AD_2, AD_3}_{\text{growing in size}}}$ $\mathcal{V}_3$ - - - - - -

Crypto Currences based on Blockchain.
1. Anonimity ??? Monero : Transaction Sender Receiver

1. Anonimity ??? Monero : Transaction Sender Receiver

		Transaction	Sender	Receiver
Monero	Anonimity	+	+	+
Bitcoin, Ethereum:	Anonimity	−	+/−	+/−

homomorphic method → +

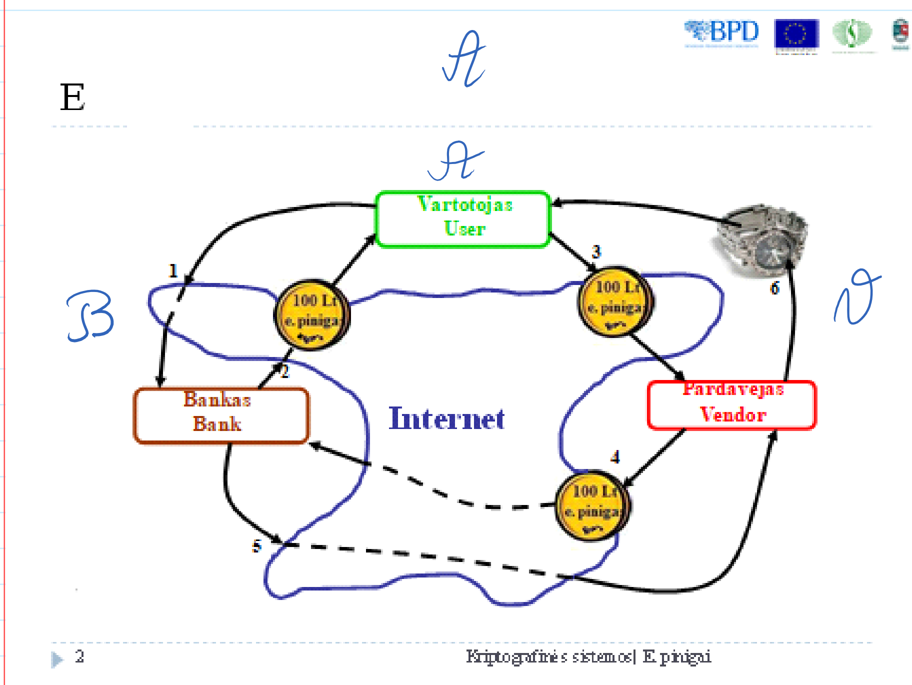
Dan Boneh

Bitcoin addr. (Addr.)
Ethereum addr (Addr.)

BTC : $F(PuK) = Addr.$

Eth : — " —

$\underbrace{Tx1, Tx2, \ldots, TxN}_{Addr_i}$



e-money anonimity

A : 50 claims to withdraw e-money from B.

$m_1 = 100, m_2 = 100, \ldots, m_{50} = 100.$

$t_1 \leftarrow rand_i, t_2 \leftarrow rand_i, t_{50} \leftarrow rand_i.$

$m_1' = m_1 \cdot t_1^e \bmod n, \ldots, m_{50}' = m_{50} \cdot t_{50}^e \bmod n.$

2% of A ... $m_1', m_2', \ldots, m_{50}'$ → B: $m_i' \leftarrow rand\{m_1', \ldots, m_{50}'\}$

2% of $\mathcal{A}$ cheating $\xrightarrow{m_1', m_2', \dots, m_{50}'}$ $\mathcal{B}$: $m_i' \leftarrow rand\{m_1', \dots, m_{50}'\}$

$\xleftarrow{m_1', \dots, m_{i-1}', m_{i+1}', \dots, m_{50}'}$

$Pr = \frac{1}{50} = 0.02$

$\xrightarrow{t_1, \dots, t_{i-1}, t_{i+1}, \dots, t_{50}}$ If $m_1' = m_1 \cdot t_1^e \bmod n$

$\xleftarrow{\sigma_i'}$ $Sign(PrK = d, m_i') = (m_i)^d \bmod n = \sigma_i'$

By collecting all m_j, $j = 1, 2, \dots, i-1, i+1, \dots, 50$,
$\mathcal{B}$ verifies: 1) if all m_j has the same value?
2) if $\mathcal{A}$ account sum $s > m_j$?
If Yes then $\mathcal{B}$ blindly signs remaining value m_i'

$\sigma_i' = (m_i')^d \bmod n = (m \cdot r^e)^d = m^d r \bmod n$ — $1 \bmod \phi$

The probability for $\mathcal{A}$ to cheat is: $Pr(cheating) = \frac{1}{50}$

$\mathcal{A}$: is unmasking σ_i' and obtains

$$\sigma_i = \sigma_i' \cdot r^{-1} \bmod n = m_i^d \bmod n.$$

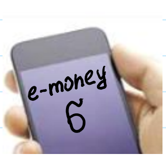
$\mathcal{A}$: verifies σ_i on m_i: $Ver(PuK = (n, e), \sigma_i, m) = T$

$$m_i = (\sigma_i)^e \bmod n = m_i^{de \bmod \phi} \bmod n = m_i^1 \bmod n = m_i$$

if $m_i < n$

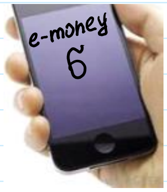
Till this place

1. Coin withdrawal Protocol 1. Untraceability.



e-wallet
$\sigma = m^d \bmod n$

e-purse
wallet



e-wallet

$\sigma = m^d \bmod n$

$m = 100\ Lt$

wallet

off-line +

on-line −

1'. Coin withdrawal Protocol 1'. Untraceability + Off-line payment.
+ Double spending preven.

A: creates Random Identification String RIS for every m'_j:
Then A encodes her name by some binary string $A = 1010$.

$x_{j1} \leftarrow \text{randbin} \rightarrow x_{j1} = 0110$

$\rightarrow x'_{j1} = A \oplus x_{j1} \rightarrow \oplus \begin{array}{c} A \\ x_{j1} \end{array} \rightarrow \oplus \begin{array}{r} 1010 \\ 0110 \\ \hline \end{array}$

$x'_{j1} = 1100$

2) Payment protocol

3) Deposit protocol

A computes:

$x_{j1}, x'_{j1};\ x_{j2}, x'_{j2};\ \ldots;\ x_{j,50}, x'_{j,50}.$

If x_{jk} and x'_{jk} is revealed, then
the identity of A will be revealed.

E.g. Let x_{j1} and x'_{j1} is known, then

$A = x_{j1} \oplus x'_{j1} \rightarrow \oplus \begin{array}{r} 0110 \\ 1100 \\ \hline 1010 \end{array} = A$

$y_{j1} = H(x_{j1}),\quad y'_{j1} = H(x'_{j1}).$

$m'_1 = m_1 \cdot r_1^e \bmod n, \ldots, m'_{50} = m_{50} \cdot r_{50}^e \bmod n.$

$\Pi'_1 = (m'_1; y_{11}, y'_{11}; \ldots; m'_{1,50}; y_{1,50}, y'_{1,50})$

$\Pi'_2 = \ldots$

$\ldots$

$\Pi'_{50} = \ldots$

$\xrightarrow{\Pi'_1, \Pi'_2, \ldots, \Pi'_{50}}$ B: $\Pi'_i \leftarrow \text{rand}\{\Pi'_1, \ldots, \Pi'_{50}\}$

$\xleftarrow{\Pi'_1, \ldots, \Pi'_{i-1}, \Pi'_{i+1}, \ldots, \Pi'_{50}}$

$\sim \quad \sim \quad \sim \quad \sim$

$1, \dots, '_{i-1}, '_{i+1}, \dots, '_{50}$ $\longrightarrow$

Verifies if:

1) all m_j have the same value
2) A account $s > m_j$

B blindly signs e-coin Π_i'

$Sig(PrK = d, \Pi_i') = \sigma_i'$

σ_i' $\longleftarrow$

A: unmasks σ_i' in the same way by computin σ_i on the sum m_i and hence A has e-coin Π_i consistin of the following:

$$\Pi_i = (m_i, \sigma_i, y_{i1}, y'_{i1}; \dots; y_{i,50}, y'_{i,50})$$

↑ not necessary to include since having signature σ_i the value m_i can be computed during the verification phase.

$\sigma_i = M^d \bmod n$; $M_i = 'm_i; y_{i1}, y'_{i1}; \dots; y_{i,50}, y'_{i,50}'$

$Ver(PuK = (n, e), \sigma_i, M_i) = \mathbf{T}$

Instead of Π_i we will use the notation Π of e-coin.

$$\Pi = (m; \sigma; y_1, y_1'; \dots; y_{50}, y_{50}')$$

2. Payment protocol.

A: $\xrightarrow{\Pi}$ V: Victor - vendor verifies

1) If signature on m is a valid B signature

$Ver(PuK = (n, e), \sigma, m) = \mathbf{T}$

2) If m value is equal to the price of silver wath.

3) V generates random bit string - RBS

consisting of 50 bits

$\mathcal{A}$: is taking RBS $\xleftarrow{RBS}$ E.g. RBS = '1 0 1 1, . . . , 0'
$b_1\ b_2\ b_3\ b_4 \ldots b_{50}$

and reveals either x_1 if $b_1 = 1$ or x_1' if $b_1 = 0$

x_2 if $b_2 = 1$ or x_2' if $b_2 = 0$

— — — — — — —

x_{50} if $b_{50} = 1$ or x_{50}' if $b_{50} = 0$

$x_1, x_2', x_3, x_4, \ldots, x_{50}'$ $\longrightarrow$ $\mathcal{V}$: verifies

$\mathcal{A}$: $\longleftarrow$

$$\left\{\begin{array}{l} \text{if } H(x_1) = y_1 \\ \text{if } H(x_2') = y_2' \\ \text{— — — — — —} \\ \text{if } H(x_{50}') = y_{50}' \end{array}\right\} \text{ If it is } \mathbf{T}$$

3. Deposit protocol. Vendor deposits his e-coins to his bank account.

$\mathcal{V}$: $\sigma, (x_1, x_2', x_3, x_4, \ldots, x_{50}')$ $\longrightarrow$ $\mathcal{B}$: Verifies: 1) if σ on Π is valid?

2) if the same string of $(y_1, y_1'; \ldots; y_{50}, y_{50}')$ didn't deliver to him?

If it is **T**, the $\mathcal{B}$ deposits e-coin Π to the $\mathcal{V}$ account.

4. $\mathcal{Io}$ impersonates $\mathcal{A}$ and is double spending Π.

To protect $\mathcal{A}$ honour we assume that $\mathcal{Io}$ together with Π seized also RIS $= (x_1, x_1'; x_2, x_2'; \ldots; x_{50}, x_{50}')$

$\mathcal{Io}$: $\xrightarrow{\Pi}$ $\mathcal{V}$: generates a different RBS_2,

$\mathcal{L}o$: $\xrightarrow{\;//\;}$ $\mathcal{V}$: generates a different RBS_2,

$RBS \neq RBS_2 = 1101, \ldots, 0$

$Pr(RBS = RBS_2) = 1/2^{50}$

$\xleftarrow{\;RBS_2\;}$

$\mathcal{L}o$ knows the actual RIS, hence she reveals to $\mathcal{V}$ required values

$\xrightarrow{\;x_1, x_2, x_3', x_4, \ldots, x_{50}'\;}$ $\mathcal{V}$: 1) Verifies signature σ on m

2) If m value is correct

3)
$$\left\{\begin{array}{l} \text{if } H(x_1) = y_1 \\ \text{if } H(x_2) = y_2 \\ - - - - - - - \\ \text{if } H(x_{50}') = y_{50}' \end{array}\right\} T$$

$\mathcal{L}o$  $\longleftarrow$

$\mathcal{V}$: $\xrightarrow{\;\Pi, (x_1, x_2, x_3', x_4, \ldots, x_{50}')\;}$ $\mathcal{B}$: Verifies:

1) If σ on Π is valis? T

2) If the same coin Π with the same $(y_1, y_1', \ldots, y_{50}, y_{50}')$ is already received previously: Yes

$\mathcal{B}$: discloses the identity of e-coin Π holder.

$$\begin{array}{r} \oplus \;\; x_1, x_2', x_3, x_4, \ldots, x_{50}' \\ x_1, x_2, x_3', x_4, \ldots, x_{50}' \\ \hline \vec{0}, A, A, \vec{0}, \ldots, \vec{0} \end{array}$$

$\downarrow$

$\mathcal{A}$ identity $A = 1010$

So $\mathcal{A}$ due to distraction has a problems with law enforcement.

Property: the only customer **Alice** can create and is responsible for Random Identification String - RIS during the Withdrawal protocol.

Questions:

1.Is it possible for **Alice** to modify e-coin $\prod$.

1.How vendor **Victor** can cheat against **Bank** and how it is prevented?

E-coin properties.

1.**Anonimity**.

2.**Untraceability**.

3.**Double-spending prevention**.

4.**Divisibility**.

International Association for Cryptographic Research - IACR Barcelona, 2008, announced results:

1.Divisible e-money can be trully anonymous.

2.Divisible and trully anonymous e-money grow in size during their transfers.