Variant ② hash of the message

$m = 5$
$y^2 = x^3 - 3x - 6$
$G = (1;5)$
$n = 15$
$Q = (6;4)$
$k = 2$
$p = 11$

gen. dig. sig.

Shumilov Alexander

1) First we find $(x_c, y_c) = k \cdot G = 2G = G \oplus G$

$G = (1;5)$

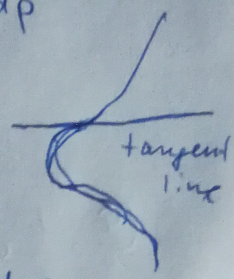
Slope: $\lambda = \frac{3G_x^2 - p}{2G_y} = \frac{3 \cdot 1 - 3}{2 \cdot 5} \equiv 0$ (no need to calc. inverse)

$\Rightarrow x_c = 0 - 1 - 1 = -2 \bmod p$

$y_c = 0(G_x - x_c) - 5 = -5 \bmod p$

$\Rightarrow x_c = -2 \bmod 11 = 9$

$y_c = -5 \bmod 11 = 6$ $\Rightarrow (x_c, y_c) = (9, 6) = kG$



$G = (x_c, x_c \cdot d + km) \bmod p$, where d: $Q = dG$

$\Rightarrow (6;4) = \underbrace{G + \ldots + G}_{d \text{ times}}$

Q — open key, d — secret key

We know $2G$ $\Rightarrow$ let's compute $3G$ and hope that we are lucky:

$3G = 2G + G = \overbrace{(9,6)}^{P} + \overbrace{(1,5)}^{Q} = R$

Slope: $\lambda = \frac{Q_y - P_y}{Q_x - P_x} \Rightarrow \begin{cases} Q_y - P_y = -1 \bmod 11 = 10 \\ Q_x - P_x = -8 \bmod 11 = 3 \end{cases}$

modulo inverse, not division

$\Rightarrow \lambda = 10 \cdot 3^{-1} \bmod 11$

$3^{-1} \cdot 3 \bmod 11 = 1$ (3 and 11 are coprime)

$\Rightarrow$ if $3^{-1} \bmod 11 = x$, then $1 = 3x \bmod 11 \Rightarrow x = 4$

$\Rightarrow \lambda = 40 \bmod 11 = 7 \Rightarrow \begin{cases} R_x = \lambda^2 - Q_x - P_x = (49 - 1 - 9) \bmod 11 = 39 \bmod 11 = 6 \\ R_y = \lambda(P_x - R_x) - P_y = (7(9-6)^3 - 6) \bmod 11 = 15 \bmod 11 = 4 \end{cases}$

Variant 2nd page Shumilov Alexander

=> indeed $Q = 3G \Rightarrow d = 3$

$\Rightarrow \sigma = (x_c, x_c \cdot d + k \cdot m) \bmod p =$

$= (9, 9 \cdot 3^{27} + 2 \cdot 5^{10}) = (9, 37) \bmod 11 = (9, 4)$

This pair is signature.

---

④ Digital right management.

It's actually great coinsidence that I got dig. rights, because 2 days ago I've read that Spotify used Blockchain to solve it's problems with copyrighting, so the use case from real life is ready.

a) First let's describe the environment. Most common (probably) example of dig. right manag. problem is media (content: music, vides, apps, ...) So such content is distributed among people. I believe that in this system there are multiple consumers and multiple content producers. So here is the answer to the a):

a) based on env. overview - no. There could be some platform that maintain the work of the system, but we cannot say that it is trusted

probably in any case there is one

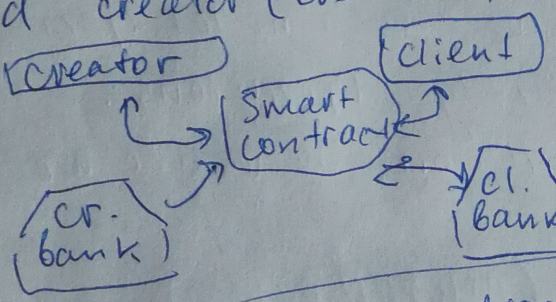
Shumilov Alexander

(4) Continuation of (#4).

b) There are multiple things to track down: creation of some content is followed by its submission to the system, then gaining rights on it. From consumer point of view there is paying for "content" that he/she wants to by (so there is transactions). Also payment to the creator is also a transaction that could be tracked.

c) In my opinion the system is insecure. The work of submission of creation lies on shoulders of creator, so he could make some intentional or non-intentional mistakes (so "paper contract" could be invalid) - could raise a problem in any part of following chain to consumer. Also example - consumer pays and because some internal error caused by human factor he wasts money and does not get anything.
And last - data insecurity. At any point system is vulnerable to attacks. So user data could be stolen (apps hacking.)

d) Smart contracts here could be used to reduce the influence of 1 person (human) on any transactions. For example between platform that connects creator and consumer, and creator (creator's bank) and consumer (consumer's bank) (to manage txs, so to say)



help

Answer is yes (6/6)

e) On 1st lecture we discussed 6 crucial points for it:
- business problem: yes, for example media content sphere
- parthers with diff. invest: yes, definetely (creat. earn money, clients spent, for ex.)
- date exch. between parthers: yes, I described it
- Many parthers modify data: yes, there are many creat., clients (agents)
- no easy fix w/t Blockchain: yes, blockchain seems to help the most (privacy, management)
- no way to rely on cent. authority: yes, discussed above.

Место для скрепки

Заключительный тур олимпиады «Турнир Ломоносова» из Перечня на 2018-2019 учебный год

09 марта 2019 11 класс

Место проведения: Москва (только для совместного написания с олимпиадой Ломоносов)

Page 4

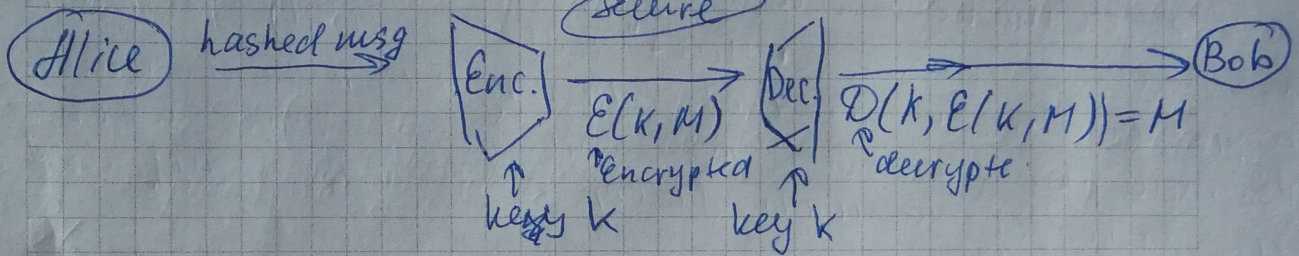
Пожалуйста, пользуйтесь темно-синей или черной ручкой, не пишите за пределами клеточек и на оборотах листов, не мните листы и не складывайте их пополам.

Shumilov Al.

Variant

(1) Block ciphers, build. blocks, example.

The question is connected with secret key cryptography. In proplem of encryption & decryption we considered so-called Block ciphers. What is block? Block - is a groop of bits with fixed length. Let's recall encr/decr. process:



So when we talk about transf. on a block, it is defined by the symmetric key.

Idea of block cipher (developed by mathematician Shannon)

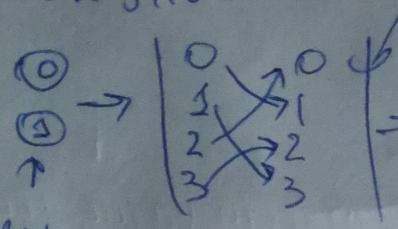
All modern and currently-used bl-ciph are based on so-called "iterated product cipher" idea. Shannon suggested to combine some similar operations to strengthen the security. Operations: substitution and permutation. On lecture we discussed Feistel example.

Substitution

Let's assume we have a message (input.) We present first it in bits form. Then we assume general "permutations" on them - substitute actually more of a substitution

Variant — Shumilov Alexander

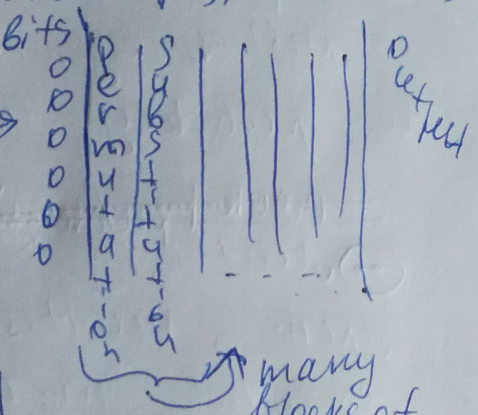
one message with another message. part
On slide we had a picture, I'll try to recreate it



2-bits example.

Note, that in ideal situations such box should be very large, but complexity in memory consuption is pretty high (biggest problem): if we have m bits, substit. to be stored – 2^m (large).

Permutation Idea - combine permutation with substitutions. Permutation is easier: we just change the order of bits in message. Difference with previous operation in substitution we should check all possible messages in order to reconstruct actual substitution. So permutation is faster (in a sence of comp. memory consump.), but less
lighter
secure.



→ (PSPSPS... such type.

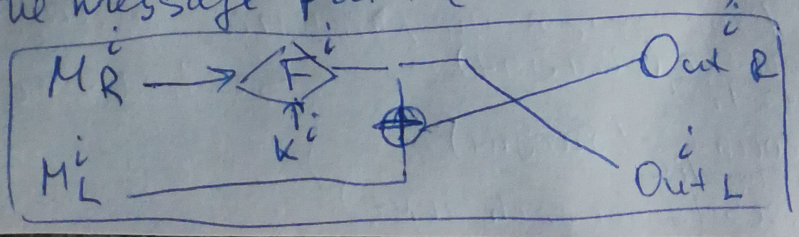
Subst. box + Permut. box:

Also we talked about role of key in choice of substitution (2 variants that depends on a key: $|S| = |S_1 \| S_0|$

key chooses

Example: Feistel cipher

> Message is been splitted in 2 parts: M_R, M_L
> Feist. Function - for so-called Feistell cell, that depends on the message part (non-linear) and the key



→ 1 block → applic. segment

Out R - new M_R
Out L - new M_L

скрепить здесь

Олимпиада «Курчатов» - 2019

Финальный этап по физике, 9 марта

11 класс

9217705057 код участника

Variant

Page 6

Shumilov D.

(3) bitcoin tx-s. Def: TX - transfer of bitcoin value that is broadcast to the network and collected into blocks

a) TX types

- coinbase tx - 1st trans. present in block that is created by a miner
- P2PKH (pay to public key hash) } for sending bitcoins to
- P2SH (pay to script hash) } bitc. addresses
- P2PK (pay to public key) } for more

P2PKH - majority of txs nowadays contains hash of public key (as it said in the name)

P2SH: script hashing

P2PK - as far as I understand, it's form is simpler than previous one (shorter because of a way of storing the public key, in p2pkH we store public key hash, not pub. key itself). Generally Less secure, aren't used in modern systems

~~- p2pk (pubkey) - si~~

- multisig - ~~require~~ before output could be spent, multisig requires a number of signatures - so-called m-of-n ≤ N of ~~public~~ given pub. keys: min. number of sig. which should match with pub. key for success
- Null data and - by wit (P2WPKH, P2WSH), W = witness

в) TX structure. Let's briefly look at structure:

TX consists of: - version (is 1 currently)
- flag (indicates the presence of data)
- in-counter (VarInt)
- Inputs list
- out-counter (VarInt)
- Output list
- Witnesses (1 for each input)
- locktime

Page 7

In detailed scheme:

4 bytes	Input: No of inputs	Tx id	Utxo output	Script size	Sig Script	Seq UB	Output: N of outputs	Btc value	Pub script	UB. Locktime

↑ prevent others from spending the outputs

Tx Structure

---

c) Bitcoin emission and circulation

First, let's compare Btc with normal physical currency.

In normal case currency is controlled by central bank organization and should match the increase in amount of goods to exchange/trade in order to organize stable good prices. It means, that CB could actually print money. It was the case of centralised economy.

In Btc case there's no authority to regulate it. Currency is created by the nodes of a peer-2-peer network. Rate of it is defined by Btc algorithms

The thing with Btc is that number of Btc in existence will not exceed 21 million, because of geometrical nature of decrease in Not Btc generated per block (and Btc are created each time when a user discovers a block)

It happens because of adjustment of Block creation rate.

generation and circulation