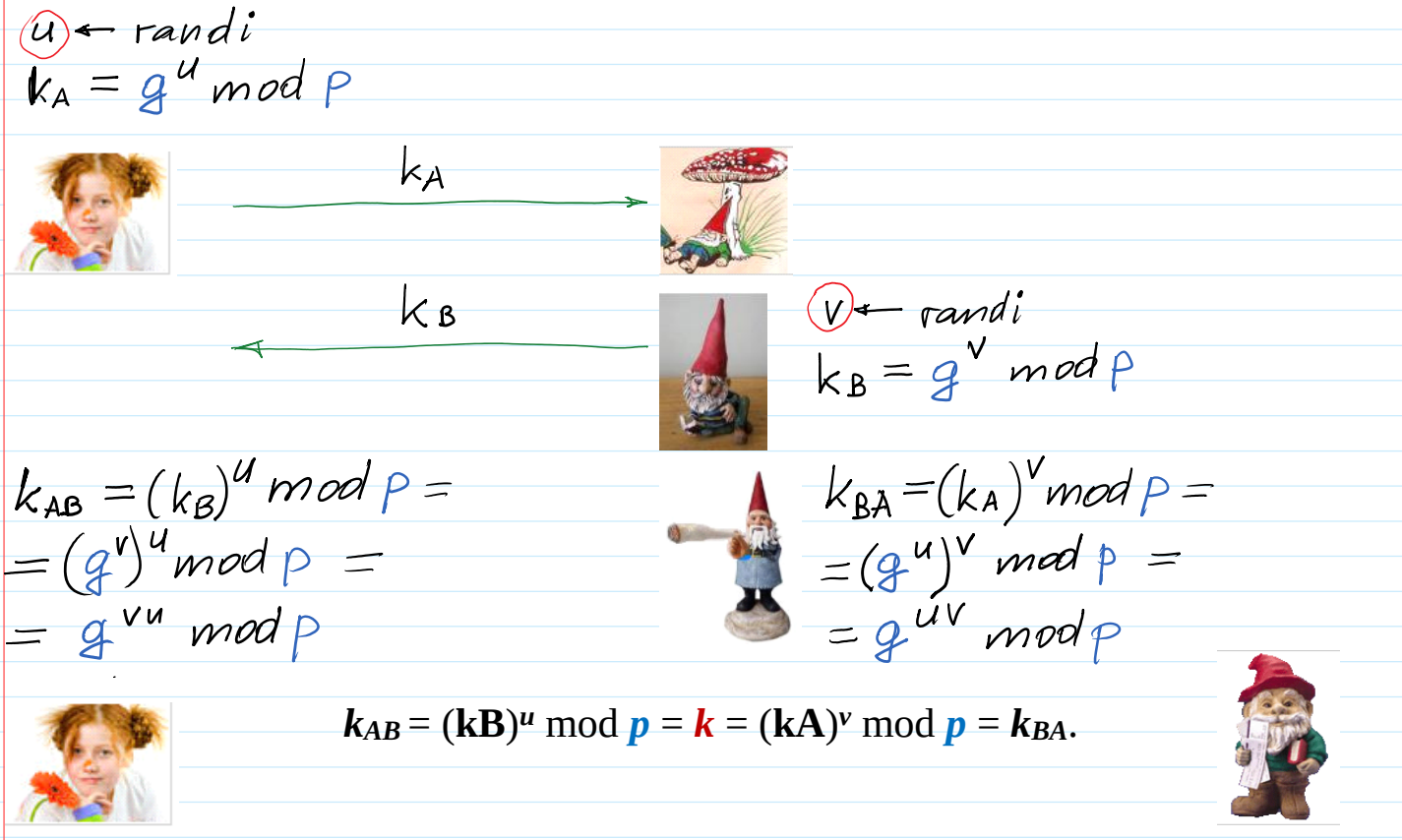
Public Parameters **PP** = (**p**, **g**): >> p=strongprime(24)
p=15728303; **g**=5;
p - strong prime; **g** - generator.

Private key **PrK** and public key **PuK** generation for **Alice** and **Bob**.

>> x=randi(p-2)	>> y=randi(p-2)
x = 13426057	**y** = 13426057
>> a=mod_exp(g,x,p)	>> b=mod_exp(g,x,p)
a = 2045067	**b** = 2045067



$$k_{AB} = (\mathbf{kB})^u \bmod p = k = (\mathbf{kA})^v \bmod p = k_{BA}.$$

http://crypto.fmf.ktu.lt/xdownload/

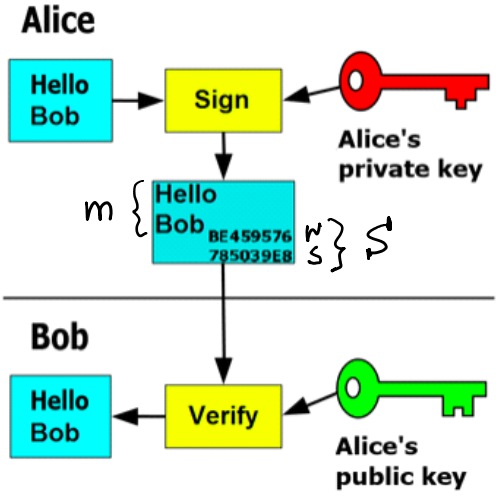
- Euronews 17-03-2015 15-38 CET_150316_HTSU_121B0-172837_E.mp4

http://www.euronews.com/2015/03/17/internet-banking-a-hacker-s-ideal-target/

Like Swiss Emmental cheese, the ways your online banking accounts are protected might be full of holes.
According to internet security software developer Kaspersky, the number of cyberthreats reached record levels in 2014.
One in three computers or mobile devices were subjected to at least one web attack over the year.
Particular targets are companies or individuals using internet banking.
In January, a Swiss firm lost an estimated one million euros in an online financial transaction that was hacked.
The victim, an accountant at the company, was unaware of what was going on.

It started when he opened an email containing an attachment infected with a virus. Once they had taken control of his computer, all the hackers had to do was wait for him to connect online with his bank.
"When he tried to connect to his bank online, he activated the "Trojan horse". A message appeared asking him to hold. For 20 or 30 minutes, he wasn't able to use his computer at all. During that time, the pirates took control of the computer and carried out several money transfers onto foreign accounts," says Frederic Marchon, spokesman for the Fribourg Police.
Plenty of viruses allowing that kind of illegal activity are available on the internet. The most updated versions are available for just over 1,000 euros on the darknet.
The hacker gets a warning as soon as someone connects with their bank online using an infected computer.
This IT expert explains how it works: "I can monitor all the computers I have successfully hacked, and I can see precisely, among them, how many are currently banking online and therefore vulnerable. So here, there are two which are currently connected," says IT expert Cedric Enzler.
Faced with a growing number of cyber attacks on companies, Switzerland has set up an emergency centre to track the attacks and analyse them. But the nature of the centre means they cannot provide with any names or figures.
"It's a really big problem. You've got to realise that anyone who wants to do harm and wants to make money that way will automatically turn to e-banking," says IT security expert Max Klaus.
For this professor at the Bern University of Applied Sciences, there's another big problem with this kind of cyber attack: most of the tools we use for internet banking like calculators or smartphone applications designed to read cryptograms are vulnerable to hacking.
"From an electronic point of vue, internet banking is safe. We use secure channels using SSL encryption. The problem comes from the client's computer, its use no longer guarantees a secure connexion. Whether it's a computer or a smartphone, hackers can take control and security is compromised," says Professor Reto Koenig.
None of the banks contacted agreed to answer to our questions on camera.
Swiss banks warn their clients about security problems linked to the use of internet in their general conditions – a warning which often comes with a clause clearing the bank of any responsibility in the event of an attack.
"The client is a victim twice over. First, he's the victim of a crook, and then he has hardly any chance to defend himself because of the general conditions in his contract. Sometimes, there are agreements between banks and clients but unfortunately, most of the time, these agreements are kept secret, they are confidential, so it's hard to find out what the procedure is, which is of course detrimental to the client," says Mathieu Fleury, of the Swiss consumer's rights association.
A coordinated cyber security taskforce and response scheme, aimed at providing cyber security services for small and medium enterprises in Europe, is to begin pilot deployments in 2015, starting in the UK, the Netherlands and Belgium.
EU authorities are concerned about the vulnerability of SMEs because they employ two-thirds of Europe's workforce.
More about:

- Banking
- Internet
- Security
- Switzerland



$PP = (p, g)$

$sig(PrK_A, K_A) = S'_A = (r_A, s_A)$

$1 < k_A < p-2$

k_A, S'_A

$\{PrK_A, PuK_A, PuK_B = b\}$

$\{PrK_B, PuK_B, PuK_A = a\}$

B: 1) Verifies signature S'_A on K_A:

$g^{s_A} = r_A \cdot a^{k_A} \bmod p$

k_B, S_B

k_B, S_B ←

on K_A:

$g^{S_A} = r_A \cdot a^{k_A} \bmod p$

2) Computes k_B

$v \leftarrow randi\,(p-2)$

$k_B = g^v \bmod p$

3) Signs k_B:

$Sig(PrK_B, k_B) = S_B = (r_B, S_B)$

A: 1) Verifies signature S_B on k_B

$g^{S_B} = r_B \cdot b^{k_B} \bmod p$

2) Computes common secrec key k_{AB}:

$k_{AB} = (k_B)^u \bmod p = (g^v)^u \bmod p$ ⇓ $g^{vu} \bmod p$

$k_{BA} = (k_A)^v \bmod p = (g^u)^v \bmod p$ ⇓ $g^{uv} \bmod p$

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

Lo: $z \leftarrow randi\,(p-2)$

$e = g^z \bmod p$

$t \leftarrow randi\,(p-2)$

$k_z = g^t \bmod p$

$Sig = (z, k_z) = S_z = (r_z, s_z)$

k_z, S_z

$Puk = e$

B: 1) Verifies S_z on k_z: using Lo declared $Puk = e$

2) Computes k_B

3) Signs k_B computing $S_B = (r_B, S_B)$

k_B, S_B ←

$k_{zB} = (k_B)^z \bmod p$

$k_{BZ} = (k_z)^v \bmod p$

$k_{zB} = k_1 = k_{BZ}$

M – message created by Lo

Using symmetric encr. method, e.g. AES-128 or (192, 256 bits)

c_1, S_1

B:

1) Verifies signature

e.g. AES-128 or (192, 256 bits)

$E(k_1, M) = AES_{128}(k_1, M) = c_1$

$h = H(c_1) : >> h = hd26('c_1')$

$Sig(z, h) = S_1 = (r_1, s_1)$

$c_1, S_1 \rightarrow$

1) Verifies signature S_1 on c_1 :

$h' = H(c_1)$

$Ver(e, S_1, h') =$ Yes

2) Decrypts ciphertext c_1 using agreed secret key k_1

$AES_{128}(k_1, c_1) = M$

This technique is named as signcryption paradigm: encrypt & sign.

it has some benefits as compared with sign & encrypt paradigm.

Encrypt & sign paradigm is resistant to so called chosen ciphertext attack - CCA : it is a strongest attack for encryption methods.

The weaker attack is:

chosen plaintext attack - CPA.

CPA : using some set of chosen plaintext / ciphertext pairs.

CCA : using some set of chosen ciphertexts / plaintext pairs.