100_008 AKAP Mini-https

https://0x0.art/

„Kriptografinių sistemų“ modulio P170M100 koliokviumas vyks Lapkričio 8 d., 17:30 nuotoliniu būdu per Zoom.
Jums reikės išspręsti 2 uždavinius iš
https://imimsociety.net/en/14-cryptography
DH-KAP ir MiM Attack.
Prisijungus prie svetainės reikia prisiregistruoti, panašiai kaip registruojatės į eParduotuvę tiktai pateikę pirmą Pavardės raidę taškas Vardas, t.y. P.Vardas, P.Vardas
Galite pateikti savo tikrą e-paštą, tačiau adresą galite pateikti bet kokį.
Po to gausite 10 Eur virtualių pinigų, už kuriuos galėsite pirkti minėtus ir kitus uždavinius.
Dėmesio, vienu metu pirkite tik 1 uždavinį, o jį išsprendę, pirkite kitą.
Jei uždavinį išspręsite sėkmingai, paspauskite mygtuką [Get Reward].
Jūsų sąskaita padidės dvigubai tiek, kiek sumokėjote, galite pasitikrinti, o papildomai manes informuoti nereikės.
Prieš koliokviumą Jūs galite spręsti uždavinius kiek norite kartų.
Per koliokviumą galite naudotis papildomais informacijos šaltiniais.

Paskutinę semestro savaitę Jums reikės paruošti pranešimą, pristatant kursinį darbą (KD) pasirinkus temą iš mano Google drive
https://docs.google.com/document/d/1bPmbwmzB2nY-vc_2APPUfO6TnYs1XrjS/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true
Lentelėje pasirinktą temą Jūs pažymėkite Pavardės pirmąja raide taškas Vardas, t.y. P.Vardas.
Keli studentai gali rinktis tą pačią temą mane apie tai mane informuodami e-paštu (žemiau).
Tai bus grupinis darbas.
Reikalavimai KD yra pateikti
http://crypto.fmf.ktu.lt/xdownload/
failuose Course_Work
Pageidautina skaidres, tekstą ir žodinį pranešimą parengti anglų k.
Suzipuota KD atsiųskite į mano e-paštą
Eligijus.sakalauskas@ktu.lt
Remiantis AIS grafiku KD turi būti apgintas 16 savaitę (arba anksčiau).

Public Parameters **PP** = (**p**, **g**): >> p=strongprime(28)
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)
x =  13426057
>> a=mod_exp(g,x,p)
a = 2045067
```

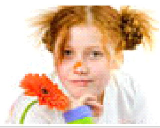
```
>> y=randi(p-2)
y =  13426057
>> b=mod_exp(g,x,p)
b = 2045067
```

```
>> p=int64(268435019)
p = 268435019
g=2;
```

```
>> p = 268435019
p = 2.6844e+08
```

$u \leftarrow randi$

$t_A = g^u \bmod p$



$t_A \longrightarrow$

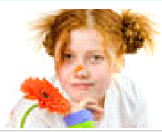
$\longleftarrow t_B$

$v \leftarrow randi$

$t_B = g^v \bmod p$

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

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



$$k_{AB} = (t_B)^u \bmod p = k = (t_A)^v \bmod p = k_{BA}.$$

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/

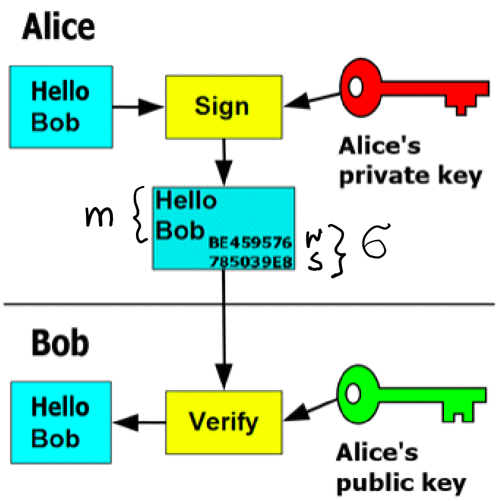
Like Swiss Emmental cheese, the ways your online banking accounts are protected might be full of holes.
According to internet security software developer Kaspersky, the number of cyberthreats reached record levels in 2014.
One in three computers or mobile devices were subjected to at least one web attack 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

Schnorr signature

$PP = (p, g)$



$Sign(PrK_A, t_A) = \sigma_A = (r_A, s_A)$

$1 < k_A < p-1$

$t_A, \sigma_A = (r_A, s_A)$

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

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

B: 1) Verifies signature σ_A on t_A: $g^{s_A} = r_A \cdot a^{t_A} \bmod p$

2) Computes t_B

$v \leftarrow randi(p-1)$

$t_B = g^v \bmod p$

3) Signs t_B:

$Sig(PrK_B, t_B) = \sigma_B = (r_B, s_B)$

$t_B, \sigma_B = (r_B, s_B)$

A: 1) Verifies signature σ_B on t_B

$g^{s_B} = r_B \cdot b^{t_B} \bmod p$

2) Computes common secret key k_{AB}:

$k_{AB} = (k_B)^u \bmod p = (g^v)^u \bmod p$ | $k_{BA} = (k_A)^v \bmod p = (g^u)^v \bmod p$

$k_{AB} = (B) \bmod p = (g) \bmod p \;|\; k_{BA} = (A) \ldots (g) \ldots$

$g^{vu} \bmod p \equiv g^{uv} \bmod p$

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

Zo: $z \leftarrow randi(p-2)$

$e = g^z \bmod p$

$i \leftarrow randi(p-1)$

$t_z = g^i \bmod p$

$Sign = (z, t_z) = \sigma_z = (r_z, s_z)$

$\xrightarrow{t_z, \sigma_z}$ $PuK = e$

B: 1) Verifies S_z, on k_z: using Zo declared $PuK = e$

2) Computes t_B

3) Signs t_B computing $\sigma_B = (r_B, s_B)$

$\xleftarrow{t_B, \sigma_B}$

$k_{ZB} = (t_B)^i \bmod p$

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

$$k_{ZB} = k_1 = k_{BZ}$$

M - message created by Zo

Using symmetric encr. method,

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

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

$h = H(c_1)$:>> $h = hd28('c_1')$

$sign(z, h) = \sigma_1 = (r_1, s_1)$

$\xrightarrow{c_1, S_1}$

B:

1) Verifies signature σ_1 on c_1:

$h' = H(c_1)$

$Ver(e, \sigma_1, h') = Yes$

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.

... 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.

```
% AES128(in,kh32,NR,fun) Advanced Encryption Standard symmetric cipher with key length of 128 bits
%                        Encryption is performed for 1 block of length 128 bits or 16 ASCII symbols
%
% in - plaintext/ciphertext of string type: maximum 16 symbols or shorter
%
% kh32 - shared secret key in hexadecimal number of length=32 (128 bits)
% kh32 can be obtained when shared decimal key k is given using commands:
%      >> k=int64(randi(2^28))
%      k = 160966896
%      >> kh32=dec2hex(k,32)
%      kh32 = 000000000000000000000000099828F0
%
% NR - Number of Rounds (e.g. Nr = 10)
%     The smaller NR, the lower security of encryption but the speed of encryption is higher
%     The least number of NR is 1 and in this case security lack is evident
%
% fun - letter determining either encription: fun='e' or decryption: fun='d' functions
%
% Encryption example:
% >> in = 'Hello Bob';
% >> kh32 = '000000000000000000000000099828F0';
% >> NR = 1;
% >> C = AES128(in,kh32,NR,'e')

>> in = 'Hello Bob'
in = Hello Bob
>>  kh32 = '000000000000000000000000099828F0'
kh32 = 000000000000000000000000099828F0
>> NR=1
```

NR = 1

>> C = AES128(in,kh32,NR,'e')

ASCII_e = WNd,bcSY

C = 2457dc4e24642c 620a63ef53ebcfc759

Dh = AES128(C,kh32,NR,'d')

Out = 0000000000000048656c6c6f20426f62

Dh = Hello Bob

No	Pavardė vardas	P.Vardas	Grupė
1.	Abraitis Steponas	A.Steponas	MGTMM-2
2.	Antanaitytė Kamilė		MGTMM-2
3.	Antanavičius Lukas		IFM-2/3
4.	Astrauskas Dominykas		IFM-2/3
5.	Baranauskis Dominykas		IFM-2/3
6.	Dovydaitis Ignas		MGTMM-2
7.	Genienė Simona		IFM-2/3
8.	Gindriūnas Marius		IFM-2/3
9.	Izokaitytė Ugnė		MGTMM-2
10.	Jonušas Laurynas		IFM-2/3
11.	Kriukaitė Dorotė		MGTMM-2
12.	Kryževičius Edgaras		MGTMM-2
13.	Kučinskas Vydenis		IFM-2/3
14.	Leonaitė Rūta		MGTMM-2
15.	Lukenskas Imantas		IFM-2/3
16.	Mikalauskas Giedrius		IFM-2/3
17.	Noreika Ričardas		IFM-2/3
18.	Obolevičius Mantas		IFM-2/3
19.	Sapitavičius Andrius		IFM-2/3
20.	Simanavičius Aivaras		IFM-2/3
21.	Svinkūnaitė Miglė		MGTMM-2
22.	Tručinskas Paulius		IFM-2/3
23.	Veščiūnas Laurynas		MGTMM-2
24.	Vyšniauskas Karolis		IFM-2/3
25.	Zigmantas Kęstutis		IFM-2/3
26.	Zumaras Lukas		IFM-2/3