123_005 KAP_MiMAttack-Fin

Kerchoff principle: a cryptosystem must be secure if its algorithm is publicly known and its security must rely only on the secrecy of its secret keys.

https:// --> Information Encryption --> Secure Channel --> Information Confidentiality

$\mathcal{Z}_p^* = \{1, 2 \dots, p-1\}$; p- strong prime. Multiplication $*$ mod p

$g \in \mathcal{Z}_p^*$ - is a group $\mathcal{Z}_p^*$ generator.

$\mathcal{Z}_p^* = \{g^i \mid i = 0, 1 \dots, p-2\}$

$|\mathcal{Z}_p^*| = p-1$

$\Downarrow$

$\mathcal{Z}_p^*$ - is a multiplicative group

Multiplication Tab Z11*										
*	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Z_{11}* = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

* **mod 11**

$$\begin{array}{r|l} 16 & 11 \\ \underline{11} & 1 \\ 5 & \end{array}$$

Exponent Tab Z11*											
^	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

$2^4 = 16$; $16 \bmod 11 = \boxed{5}$,

$10 = p - 1$

Exponents are computed mod$(p-1)$

9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

C.5.3 **Finding generators**.
We have to look inside Z_P^* and find a generator. How?
Even if we have a candidate, how do we test it?
The condition is that g is a generator of Z_P^* which would take $|Z_P^*|$ steps to check.
In fact, finding a generator given p is in general a hard problem.
In fact, even checking that g is a generator given p is a hard problem.
But what we can exploit is that is strong prime $p=2q+1$ with q prime.
Note that the order of the group Z_P^* is $p-1=2q$. Prime p is called a **strong prime**.

Fact C.23. Say $p=2q+1$ is srong prime where q is prime. Then g in Z_P^* is a generator of Z_P^*
iff (if and only if - tada ir tik tada) $g^q \neq$ **1 mod** p **and** $g^2 \neq$ **1 mod** p.

```
>> p=genstrongprime(28)
p = 251487959
>> q=(p-1)/2
q = 125743979
>> isprime(q)
ans = 1
```

```
>> g=randi(2^8)
>> mod_exp(g,q,p)       % neq to 1
>> mod_exp(g,2,p)       % neq to 1
```

Fact C.24. If g is a generator and i is not divisible by q or **2** then g^i is a generator.

NSA

Diffie-Hellman Raktų Apsikeitimo Protokolas - RAP
Diffie-Hellman Key Agreement Protocol - KAP

Published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

https://imimsociety.net/en/

Public Parameters - PP=(p, g) generation

1. **Public Parameters - PP=(p, g) generation.**
   Administrator generates strong prime number p
   (we use short numbers of 28 bits length using Octave function)
   >> p=genstrongprime(28).

and finds generator g of cyclic group Z_p*={1,2,3,…,p-1}.
Administrator sends public parameters **PP**=(p, g) to the users Alice and Bob.
p = 264043379; Strong prime, g=2; Generator.

2. **Alice** generates at random secret number u in the interval **$1<u<p-1$**, computes session public parameter $K_A=g^u$ ***mod*** p and sends [K_A] to Bob.

3. **Bob** generates at random secret number v in the interval **$1<v<p-1$**, computes session public parameter $K_B=g^v$ ***mod*** p and sends [K_B] to Alice.

*At this moment communications between **Alice** and **Bob** for common secret key agrement protocol are finished.*

4. **Alice** after receiving K_B computes

$$K_{AB} = (K_B)^u \bmod p = (g^v)^u \bmod p = g^{vu} \bmod p.$$

5. **Bob** after receiving K_A computes

$$K_{BA} = (K_A)^v \bmod p = (g^u)^v \bmod p = g^{uv} \bmod p.$$

6. Evidently parties agreed on the same secret key K

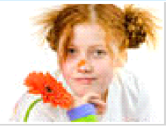
$$K_{AB} = g^{vu} \bmod p = K = g^{uv} \bmod p = K_{BA}.$$

$PP=(p,g)$

$\boxed{u} \leftarrow$ randi

$K_A = g^u \bmod p$

$\xrightarrow{K_A}$



$\xleftarrow{K_B}$

$\boxed{v} \leftarrow$ randi

$K_B = g^v \bmod p$

$K_{AB} = (K_B)^u \bmod p =$

$= (g^v)^u \bmod p =$

$K_{BA} = (K_A)^v \bmod p =$

$= (g^u)^v \bmod p =$

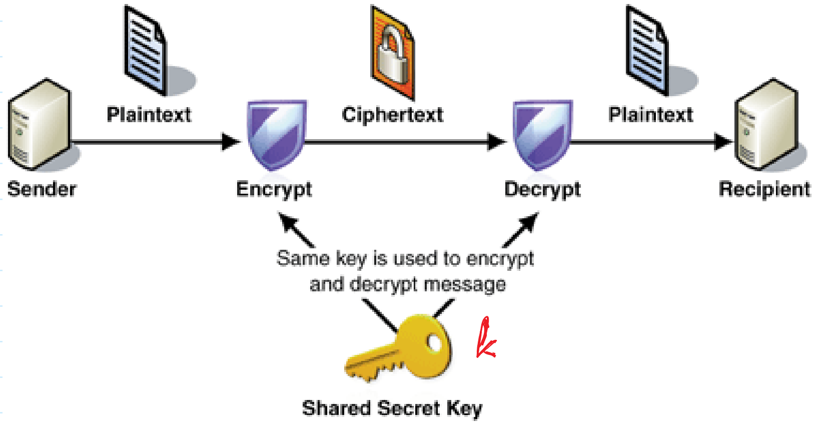
$= (g^v)^u \bmod p =$

$= g^{vu} \bmod p$

$= (g^u)^v \bmod p =$

$= g^{uv} \bmod p$

$$K_{AB} = g^{vu} \bmod p = \boxed{K} = g^{uv} \bmod p = K_{BA}.$$



Encryption with Vernam cipher

m – message to be encrypted: $|m| \le |k|$

```
>> mb = dec2bin(m);
>> kb = dec2bin(k);
```

} cb = binaryxor(mb, kb)

$$\begin{array}{rr} mb = & 1010 \\ \oplus\ kb = & 0110 \\ \hline cb = & 1100 \end{array}$$

Attention! If the same agreed secret key ***k*** is used in Vernam cipher twice for any two messages m_1 and m_2 encryption, then ***eavesdropping*** adversary can obtain an information ***m*** which is equal to bitwise XOR between m_1 and m_2. Let ciphertexts c_1 and c_2 are obtained by the following encryption

$$c_1 = m_1 \oplus k,$$
$$c_2 = m_2 \oplus k,$$

where $\oplus$ is bitwise XOR operation.

Then eavesdropping adversary computes the following data ***d***

$$\boxed{d} = c_1 \oplus c_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2 \oplus \boxed{0} = \boxed{m_1 \oplus m_2.}\ !$$

$$\begin{array}{rr} kb = & 0110 \\ \oplus\ kb = & 0110 \\ \hline & \boxed{0000} \end{array}$$

It is reckoned as a crucial insecurity since cryptanalysis of data ***d*** is significantly facilitated and both m_1 and m_2 can be disclosed.

Moreover, if any message of two m_1 and m_2 are revealed by some circumstances, say message m_2, then the other message m_1 becomes clear to the adversary by computing

$$d \oplus m_2 = m_1 \oplus m_2 \oplus m_2 = m_1 \oplus 0 = m_1.$$

$$\begin{array}{rr} mb = & 1010 \\ \oplus\ 0b = & 0000 \\ \hline & 1010 \end{array}$$

Never use the same secret key ***k*** twice in Vernam cipher!

The same secret key ***k*** can be used multiple times in standardized block and stream ciphers.

Attack "Man in the Middle" --> Impersonation --> Active Adversary

Public Parametrs PP=(p,g)

Eavesdropping adver.

Attack „Man in the middle" „Impersonation" Active adversary

"Apsimetimas"

$u \leftarrow randi$

$K_A = g^u \bmod p$

K_A

malware

pot

$\alpha \leftarrow randi$

$Z_A = g^\alpha \bmod p$

Z_A

$v \leftarrow randi$

$K_B = g^v \bmod p$

K_B

$\beta \leftarrow randi$

$Z_B = g^\beta \bmod p$

Z_B

W

Two agreed secret keys K_{AZ} and K_{ZB}

$K_{AZ} = (Z_B)^u \bmod p =$

$= (g^\beta)^u \bmod p =$

$= g^{\beta u} \bmod p = K_{AZ} = g^{u\beta} \bmod p$

$= (g) \bmod p =$

$= g^{\beta u} \bmod p = K_{AZ} = g^{u\beta} \bmod p$

$K_{ZB} = (Z_A)^{v} \bmod p =$

$= g^{v\alpha} \bmod p = K_{BZ}.$

Encryption

A: L - message to be sent to B

K_{AZ} K_{ZB}

$Enc(K_{AZ}, L) = C_L$

$\downarrow C_L$

L' - the other letter

$Enc(K_{ZB}, L') = C_L' \xrightarrow{C_L'} B:$

$Dec(K_{ZB}, C_L') = L'$

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

Authenticated D-H protocol.

1. After computing K_A A provides a proof for B that this number is computed by herself and not by anybody else.

2. $A \xrightarrow[Proof_A]{K_A} B$

3. B verifies the validity of K_A and computes K_B, B also provides a proof that number K_B is computed by himself.

$B \xrightarrow[Proof_B]{K_B} A$.

5. A verifies validity of K_B and if it is ok, then computes common secret key K_{AB}.

6. B computes common secret key K_{BA}.

Till this place

e - Signature

$A: PrK_A = (x)$ $PuK_A = (a)$ $\qquad B: PrK_B = (y)$ $PuK_B = (b)$

$PuK_A = a$

m - message

$\sigma(PrK_A, m) = s$

$\sigma(PrK_A, K_A) = s_A \xrightarrow{K_A,\ s_A} B$: 1. To verify s_A on K_A

$$\vartheta(PuK_A, s_A, K_A) = \begin{cases} 1, \text{OK} \\ 0, \text{Fail} \end{cases}$$

Zo: $\xrightarrow{Z}$ B

Bob I'm A and I'm sending you my

$PuK = Z$

PKI - Public K Infrastructure

Verisign : TTP PuK_{CA}, PrK_{CA};

Certification Authority

2. computes common secret key k

Protokolo vykdymas:

1: $u \leftarrow randi$

$A = g^u \bmod p$

$s_A = \sigma_{PR_A}(A) \xrightarrow{A,\ s_A} B \qquad Cert(VR_A)$

2. B : patikrina parašą s_A

$\vartheta_{VR_A}(s_A) = \begin{cases} \text{True} \oplus \\ \text{False} \end{cases} \rightarrow Cert(VR_A)$ verification +

$v \leftarrow randi$

$K_{BA} = (A)^v = g^{uv} \bmod p$

$B = g^v \bmod p$

$s_B = \sigma_{PR_B}(B) \xrightarrow{B,\ s_B} A \qquad Cert_B$

A: $\vartheta_{VR_B}(B, s_B) = \begin{cases} \text{True} \oplus \\ \text{False} \end{cases} \rightarrow Cert(VR_B)$ verification +

$K_{AB} = (B)^u \bmod p = g^{vu} \bmod p$

$K = K_{AB} = K_{BA}$

$\mathcal{L} : (PR'_A , VR'_A)$ $\mathcal{L} : (PR'_B , VR'_B)$

$\mathcal{A} : (PR_A , VR_A)$ $\mathcal{B} : (PR_B , VR_B)$

$CA : (PR_{CA}, VR_{CA})$

$\sigma_{PR_{CA}} (VR_A) \Rightarrow Cert(VR_A)$

$\sigma_{PR_{CA}} (VR_B) \Rightarrow Cert(VR_B)$

Public Key Infrastructure - PKI

Security

Find: $Pr\, k_A = x$, when given p, g, a

$$a = g^{x} \bmod p$$

It is infeasible to find x if p is large enough: $p \sim 2^{2048}$

$$\log_g a = \log_g g^x \bmod p = x \log_g g \bmod p =$$

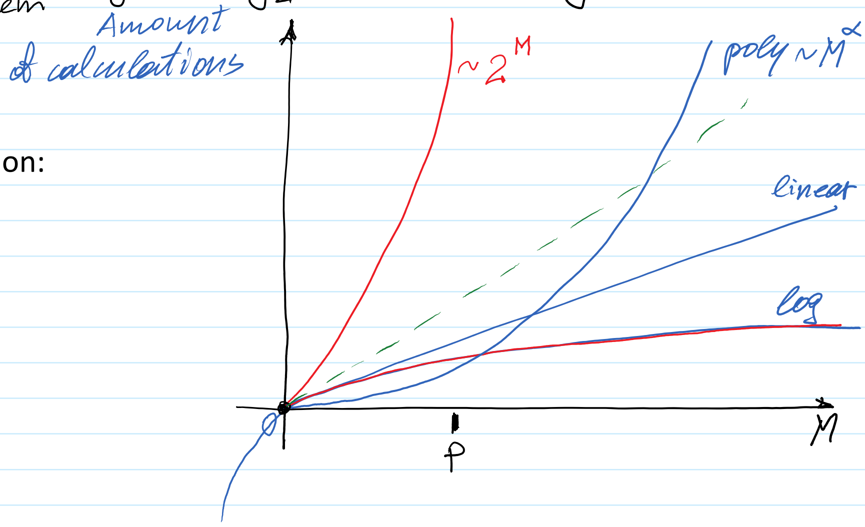
$$= x \cdot 1 \bmod p = x \bmod p = x$$

$$\boxed{x = \log_g a \bmod p}$$

Discrete Logarithm Problem
DLP

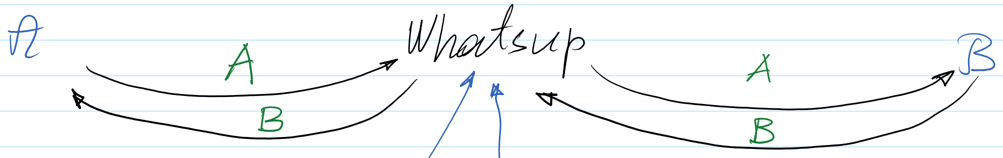
Computation Complexity
Theory

M-records → ordering problem $\log_2 M \sim O(\log_2 M)$



Secure parameter value determination:
P ~ 2^{2048}

Telegram
Whatsup



$$K_A = B^u \bmod p = K = K_B = A^v \bmod p$$

$u \leftarrow$ rand

Man-in-the-Middle

Backdoors

$v \leftarrow$ rand