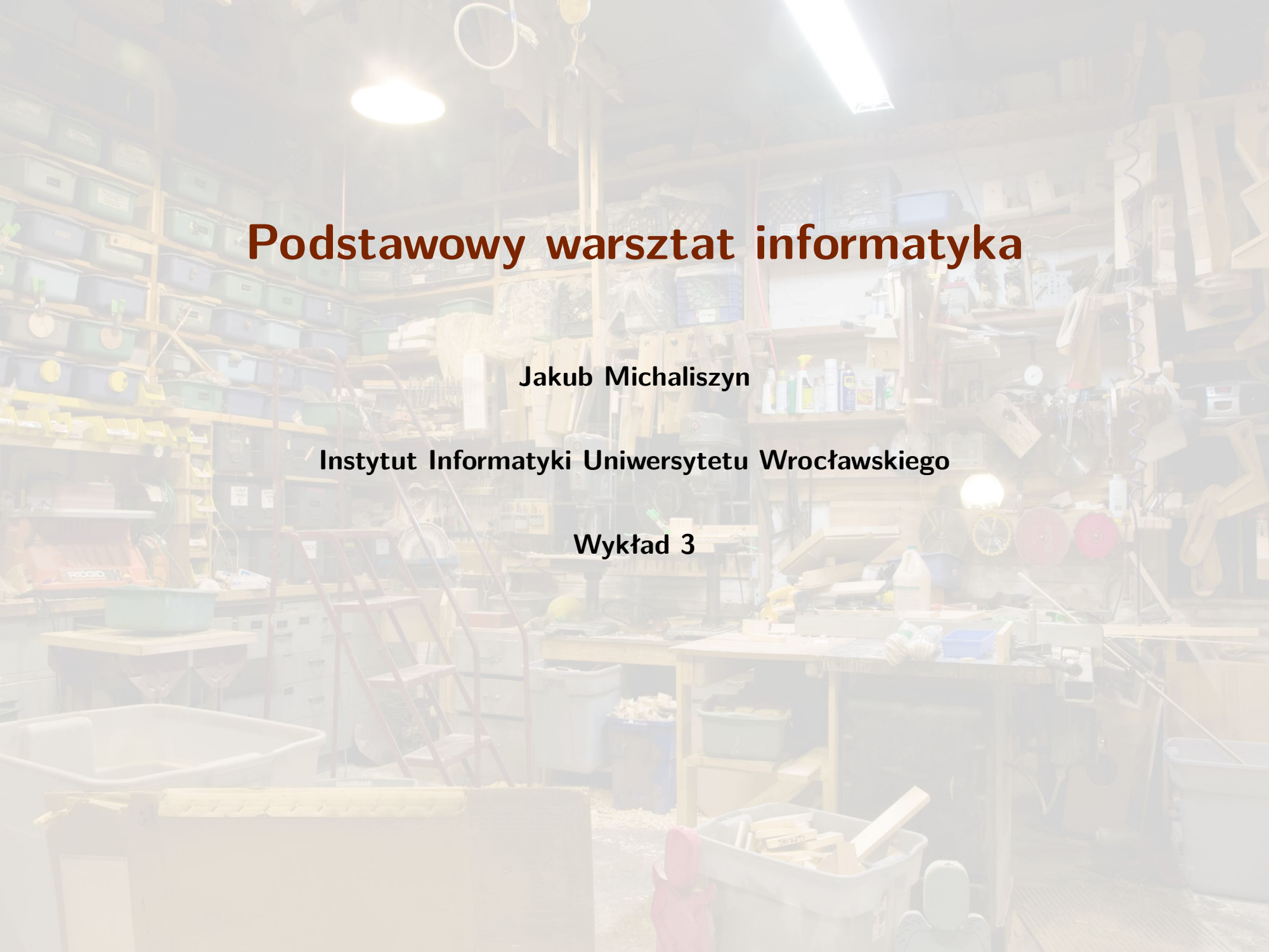


Podstawowy warsztat informatyka

Jakub Michaliszyn

Instytut Informatyki Uniwersytetu Wrocławskiego

Wykład 3

Sprawy organizacyjne

- Lista 4 będzie duża.
- Lista 5 będzie off-line.
- Lista 6 - głosowanie; wynikiem dużo:12 ustalono, że będzie off-line.

Dotychczas przerobiliśmy

- Operacje na plikach.
- Konta użytkowników.
- Tworzenie i zabijanie procesów.

Warto jeszcze wspomnieć o:

- Używaniu $*$ i ? w poleceniach.
- Plikach ukrytych (nazwa od kropki).
- Znakach “.

ssh

ssh umożliwia szyfrowane łączenie się z innymi komputerami

ssh

```
$ ssh ii.uni.wroc.pl
The authenticity of host 'ii.uni.wroc.pl (156.17.4.11)'
can't be established.
ECDSA key fingerprint is SHA256:8B
+U6a165kARogRiq90n1Jv41p+IZhBlEBinyRwOmJs.
Are you sure you want to continue connecting (yes/no)?
```

ssh

```
$ ssh ii.uni.wroc.pl
The authenticity of host 'ii.uni.wroc.pl (156.17.4.11)'
can't be established.
ECDSA key fingerprint is SHA256:8B
+U6a165kARogRiq90n1Jv41p+IZhBlEBinyRwOmJs.
Are you sure you want to continue connecting (yes/no)?

Warning: Permanently added 'ii.uni.wroc.pl' (ECDSA) to the
list of known hosts.
jmi@ii.uni.wroc.pl's password:
```

ssh

```
$ ssh ii.uni.wroc.pl
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now
(man-in-the-middle attack)! It is also possible
that the RSA host key has just been changed. The fingerprint
for the RSA key sent by the remote host is ab:cd:ef:gh
Please contact your system administrator. Add correct host
key in /home/user/.ssh/known_hosts to get rid of this message

Offending key in /home/user/.ssh/known_hosts:1
RSA host key for user.server has changed and you have
requested strict checking.
Host key verification failed.
```

scp

scp to odpowiednik ssh do kopiowania plików

```
scp Opis.txt www@ii.uni.wroc.pl:.
www@ii.uni.wroc.pl's password:
```

Po dwukropku jest ścieżka na zdalnym serwerze.
Można również kopiować w drugą stronę.

```
scp www@ii.uni.wroc.pl:fotki/* zdjecia
```

Szyfrowanie asymetryczne

```
jmi@ii.uni.wroc.pl's password:
```

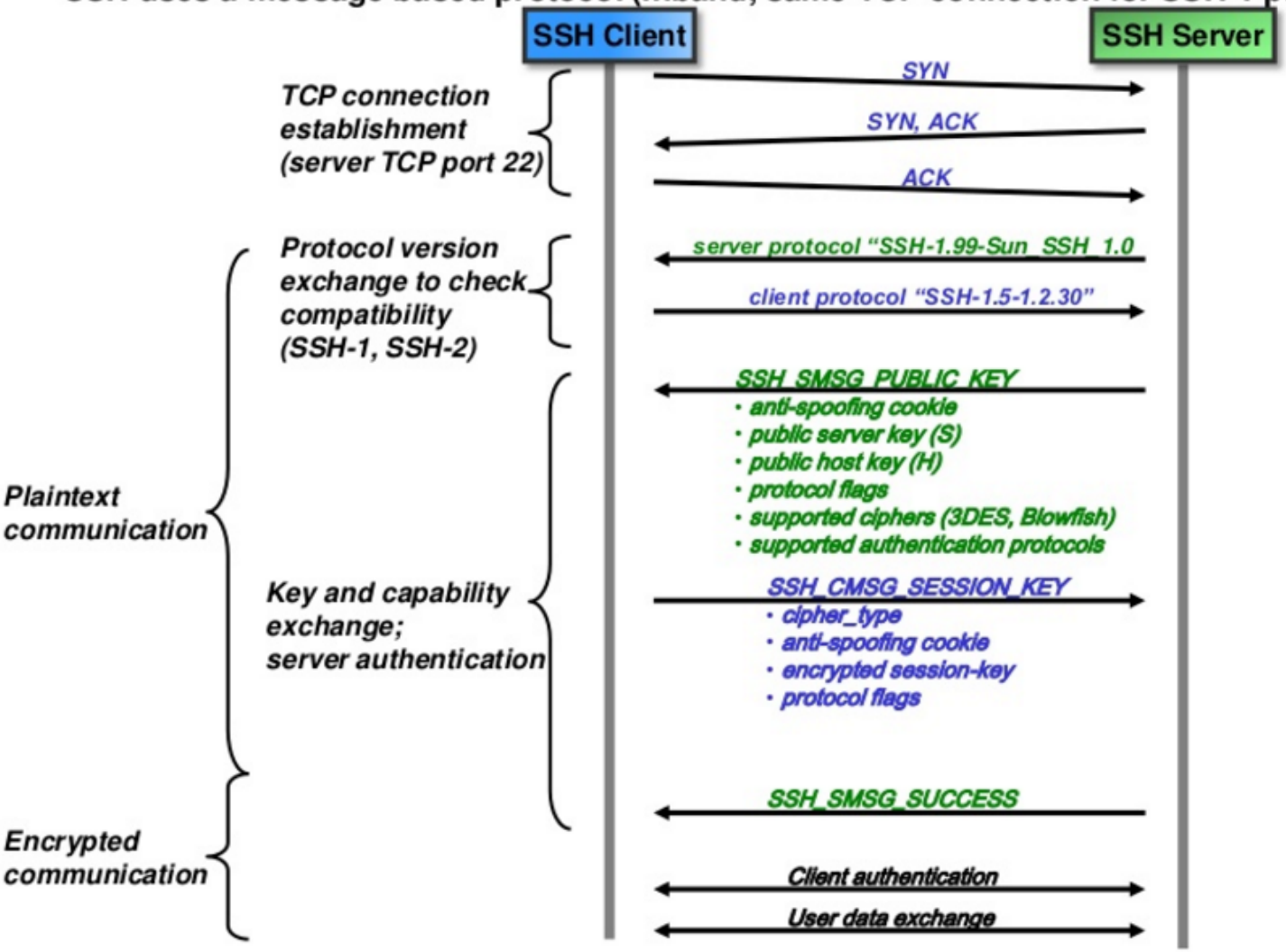
Ciągłe podawanie hasła jest uciążliwe i potencjalnie niebezpieczne.
Pomoże nam kryptografia!

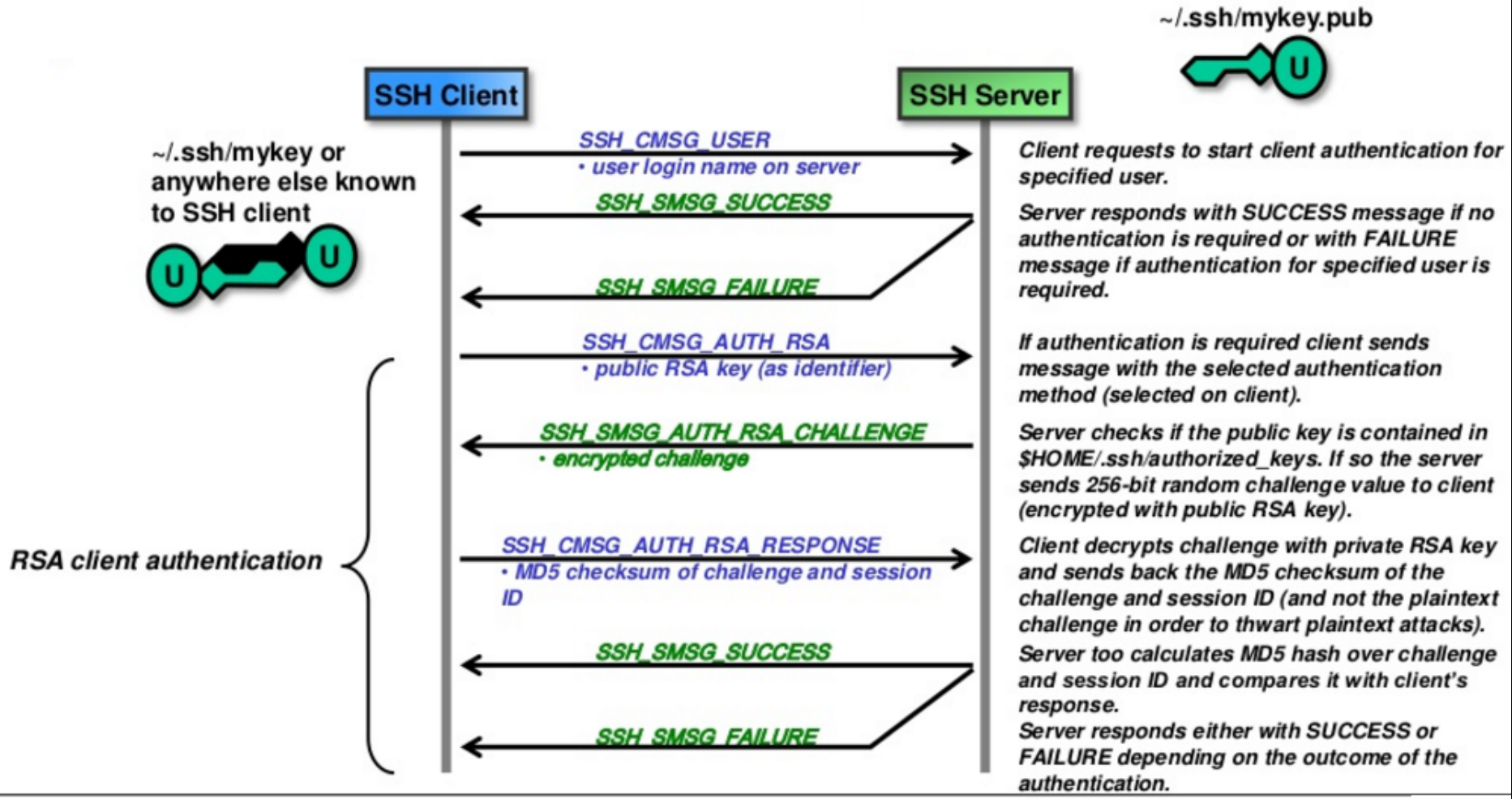
Klucze prywatne i publiczne

Użytkownik generuje dwa klucze - prywatny i publiczny.
Wiadomość zakodowaną kluczem prywatnym można odkodować tylko publicznym, i odwrotnie.
Nie da się (szybko) wyliczyć jednego klucza na podstawie drugiego.

3. SSH-1 protocol

SSH uses a message based protocol (inband, same TCP connection for SSH-1 protocol and for user data).





Klucze prywatne i publiczne

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/me/.ssh/id_rsa):
Created directory '/home/me/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/me/.ssh/id_rsa.
Your public key has been saved in /home/me/.ssh/id_rsa.pub.
The key fingerprint is:
a9:49:2e:2a:5e:33:3e:a9:de:4e:77:11:58:b6:90:26 me@host
The key's randomart image is:
+--[ RSA 2048]----+
|        ..o      |
|      (...)      |
|o=++.            |
+-----------------+
```

Wgrywanie klucza

Klucz prywatny jest naszą tajemnicą!
Klucz publiczny wgrywamy na serwer:

```
ssh-copy-id www.example.com
```

i już!

Inne ważne funkcje

Tunelowanie
Komunikacja z programami graficznymi (-X)
screen przez ssh
Hasła do kluczy i ssh-agent