Co-funded by the
Erasmus+ Programme
of the European Union

InCyT Training Modules

Information Security for Employees Unit no: (3) Week 5 Unit (Module) name: (Security at business trips)	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Mirosław Mazurek • Paweł Dymora
Learning Activity Goals	1. Wireless networks 2. VPN 3. Email encryption
Skills to be Gained	• **TS3** • **SS2**
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • MS Office365

Co-funded by the
Erasmus+ Programme
of the European Union

Brief information about the module

Description
The general outline of this module is to provide some theoretical and practical issues related to knowledge and practical skills security at business trips. You will have the possibility to protect your wireless network and use protected wireless networks with the idea of VPN. The module will also cover how to send emails securely using free PGP protocol for encrypted messages which no one can decipher without your permission.

Content of the Learning Material

1. Introduction to wireless networks. Theoretical basics: principle of operation, encryption protocols.

Earlier WEP and WPA protocols were used to secure wireless networks, but they were not resistant to hackers' attacks. The introduction of the WPA2 protocol allowed to ensure a sufficient level of security, but it does not provide full security anyway. There are many network topologies, wireless access protocols and network access acquisition techniques available, and both CPU (Central Processing Unit) and GPU (Graphics Processing Unit) computing architectures are used in network key acquisition [1,2].

WEP (Wired Equivalent Privacy) is one of the oldest IEEE 802.11 wireless encryption standards. It provides information protection based on the use of the RC4 algorithm. It has many known security vulnerabilities and has therefore been cracked multiple times. It is one of the oldest standards for securing WLAN networks (established in 1997). It does not require high computing power of the installed devices. It uses two user authentication methods: Open Authentication and Shared Key Authentication. In addition, it enables user verification based on physical MAC addresses using the ACL (Access Control List). There is a 64-bit WEP variant (based on a 40-bit key and 24-bit initialisation vector) and a 128-bit WEP variant (based on a 104-bit key). Some manufacturers have also introduced a 256-bit WEP standard [1,2].

WPA (Wi-Fi Protected Access) is another standard for encryption of IEEE 802.11 wireless networks. It was introduced to improve the level of security of WLAN networks, replacing known vulnerabilities in the WEP standard. It is based on the use of protocols: TKIP (Temporal Key Integrity Protocol) and EAP (Extensible Authentication Protocol), 802.1x standard and the MIC (Message Integrity Check) mechanism. The standard is based on the RC4 algorithm. It was implemented as an interim solution between the WEP standard and the current most secure wireless encryption

standard 802.11i. It provides work in two modes, which include: Enterprise (using a RADIUS server that manages the allocation of keys to users) and Personal (using a shared PSK key) [1,2].

WPA2 (Wi-Fi Protected Access 2) is currently the most powerful encryption standard for wireless networks (also known as 802.11i). It provides information protection based on the use of the AES (Advanced Encryption Standard). It was introduced to improve the level of security of WLAN networks, replacing known vulnerabilities in the WEP standard and the interim WPA standard. It implements the 802.1x protocol improving the control of user access to the network. It provides work in two modes, which include: Enterprise (using a RADIUS server that manages the allocation of keys to users) and Personal (using a shared PSK key) - often used in home solutions today [1,2].

The WEP algorithm is the least secure encryption standard for IEEE 802.11 wireless networks. It has been cracked many times by various methods due to the many currently known vulnerabilities in the security aspects of the algorithm. The main disadvantages of the standard include[3]:

- Lack of a defined key management system (often one network key is used by all nodes of a wireless network);
- Insufficient bit size of the network key (the first version of the WEP standard introduces 40-bit keys);
- Insufficient bit size of the IV initialization vector (the WEP standard introduces a 24-bit initialization vector, which turns out to be insufficient and, due to the relatively high probability of collisions with a small number of received packets, there is a possibility of a cryptographic attack to obtain the value of the WEP key);
- Weak ICV checksum based on CRC-32 linear function (there is a possibility of unnoticeable modification of the information sent in the network);
- Weak RC4 information encryption algorithm (there are too many dependencies between the network key and the result of information encryption);
- Insufficient user authentication system (there is a possibility of forging authentication messages).
- Based on the presented weaknesses of the WEP algorithm, many tools have been created to conduct attacks that test the security level of WLAN networks. The most popular attacks against WEP include:
- FMS attack - a statistical attack (developed by Fluhrer, Mantin and Shamir) on the RC4 algorithm used in the WEP encryption standard;
- KoreK attack - a statistical attack (developed by a person nicknamed KoreK) that uses several more (compared to the FMS attack) dependencies of the RC4 algorithm encryption process;
- Chopchop attack - an interactive attack, carried out in the direction of gaining access to the network by gradually decrypting one of the received packets;
- PTW attack - is a statistical attack (developed by Pyshkin, Tews and Weinmann) on the RC4 algorithm, which, thanks to the successive dependencies of the data encryption

process, significantly increases the probability of obtaining the key value with a relatively small number of received packets.

Another frequently used type of attack is the Dictionary attack. It is one of the brute-force methods of acquiring e.g. cryptographic key values in wireless computer networks. To obtain WPA/WPA2 key values, the method is based on one-way encryption and comparing entries in the dictionary with information in the captured 4-way handshake sequence. Dictionary attacks are carried out with the intention of reducing the time of obtaining key values compared to the brute-force method. The process of retrieving the key value continues until a positive result is obtained (i.e., when the entry in the dictionary turns out to be a valid key value) or until all entries in the dictionary are compared with the negative result. A negative result may indicate a high level of complexity of the key value and the need to use the brute-force method[3].

The success of this attack is the selection of an appropriate dictionary. Dictionary is a text file used in the case of dictionary attacks to obtain, for example, cryptographic key values. It contains a list of appropriately prepared items that may constitute the key value sought. The use of dictionaries in the case of force attacks allows to significantly reduce the set of examined values, which may result in speeding up the process of acquiring the cryptographic key value. The content of dictionaries is built, for example, on the basis of the presented items[3]:

- a list of words appearing in national and foreign dictionaries;
- combinations of words with uppercase and lowercase letters, words spelled backwards (i.e. palindromes);
- combinations of dictionary entries with cut out vowels or consonants;
- combinations of multiple repetitions of selected names, surnames, dictionary entries;
- combinations of words with numerical values, special characters, etc.;
- a list of passwords and logins most frequently used by users;
- a list of popular companies, organizations, technical terms, proper names, etc.;
- information leaks (i.e. logins, nicknames, passwords) from various internet portals;
- combinations of adjacent keyboard characters for selected patterns (Fig. 1).

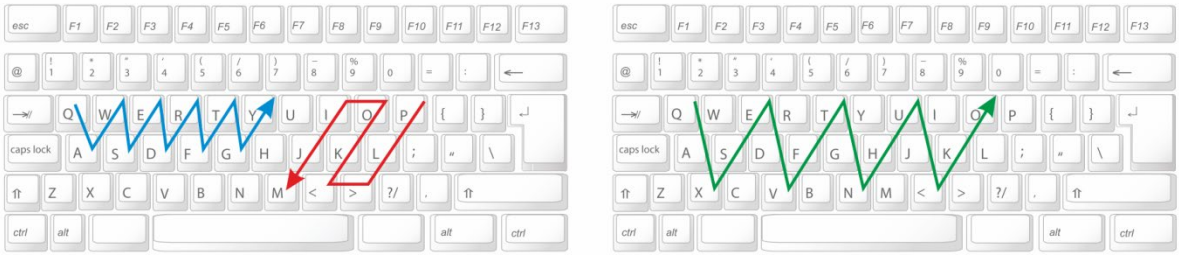


Fig. 1. Schema showing examples of network key creation patterns

The network key plays a key role in the study of network resilience. It is a sequence of characters used by network users in the authentication process. The authentication process is an

important step in protecting access to shared services and network resources from unauthorized users. Network keys are often created and managed by network administrators and may constitute the weakest link in the security of a computer network. Key values that turn out to be relatively time-consuming or impossible to break using brute-force methods in realistic time should be generated, for example, based on the rules presented[3]:

- Each wireless network managed by the administrator should be secured using a different network key;
- Each network user should use an individual network key;
- Network keys should be built on a sufficient number of characters;
- The generation of keys should be based on the maximum available character space;
- Keys should not be generated using corporate and personal information;
- Keys generation should not be based on a list of items in publicly available dictionaries;
- Network keys should be built on the basis of random sequences of characters;
- Network keys should be updated periodically;
- Currently used key values should not be associated with key values that are no longer used.

2. Virtual VPN tunnels. Theoretical basis: types, architecture, principle of operation, encryption protocols. Installation of the Open VPN programme (configuration, addressing, parameter selection, key generation).

A Virtual Private Network is a tunnel through which private network traffic flows between the sender and recipient over a public network. VPN stands for 'Virtual Private Network'. A VPN network encrypts all activities on the internet, hides the IP address, protecting the identity of the network user. A VPN connection offers secure access to applications, websites and entertainment platforms from anywhere in the world. It is possible to optionally compress or encrypt transmitted data to provide better quality or a higher level of security, thus protecting privacy within the network [4].

A secure tunnel is created by first authenticating the client with the VPN server. The server then applies an encryption protocol to all data that is sent and received. To ensure the security of each data packet, the VPN places it in an external packet, which is then encrypted by encapsulation. It ensures the security of the data during transmission and is a fundamental component of the VPN tunnel. After the data reaches the server, the external packets are removed in the decryption process [4].

VPNs can be divided into two main categories [5]:

- A remote access VPN that allows users to connect to a remote network, usually through special software.
- Site-to-site VPNs used by companies, especially large corporations. They allow users in selected locations to securely access other users' networks.

An example of a dedicated VPN development software is *RadminVPN*. In most cases it is not necessary to have a static IP address in your local network to set up a VPN tunnel. After downloading

the appropriate software, it will create an appropriate network with a static address of your computer [6].

Radmin VPN allows you to connect to two computers on two different networks. A configuration example is shown below. For easier understanding of the operation of the VPN channel, Fig. 2 and 3 shows the initial configuration of computers between which a secure channel is to be created.

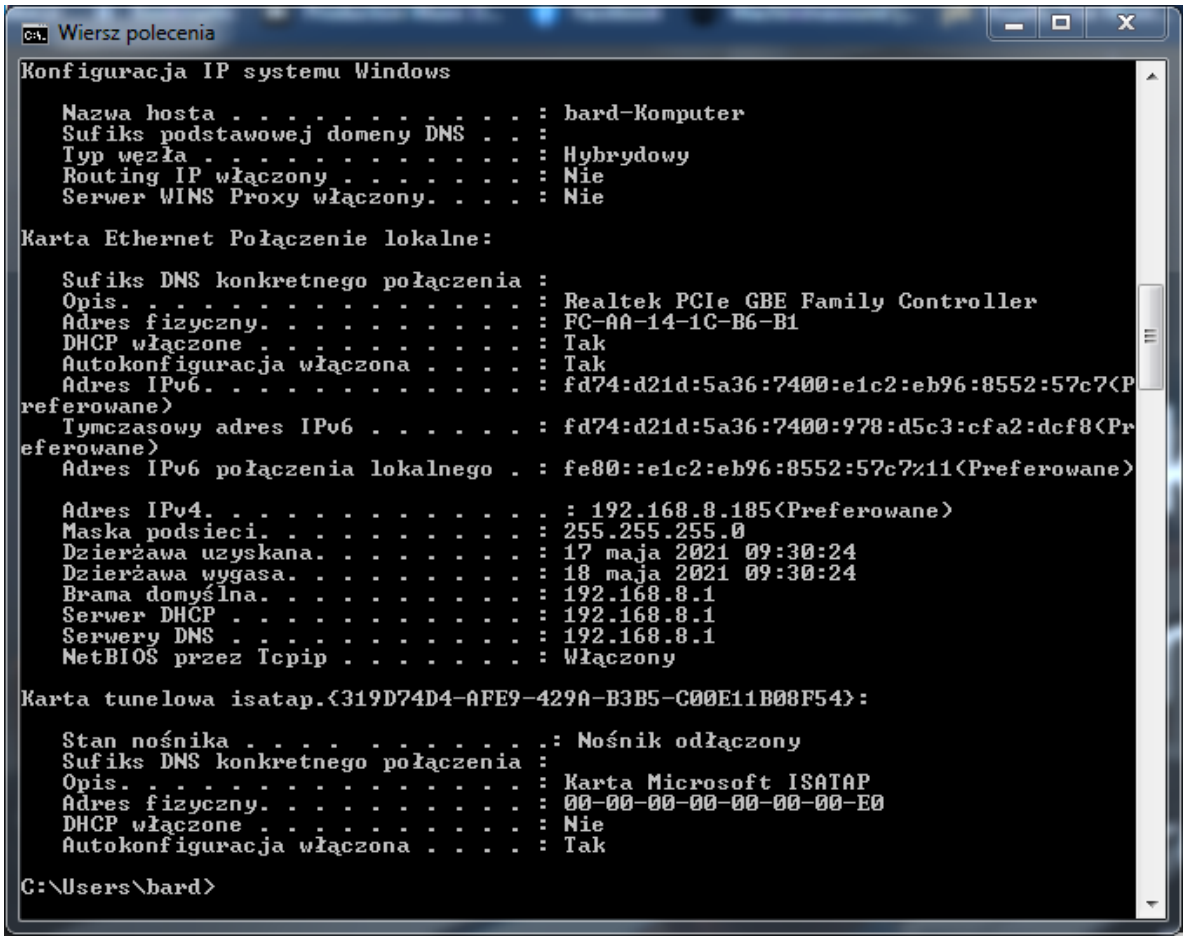


Fig. 2. Initial configuration of computers

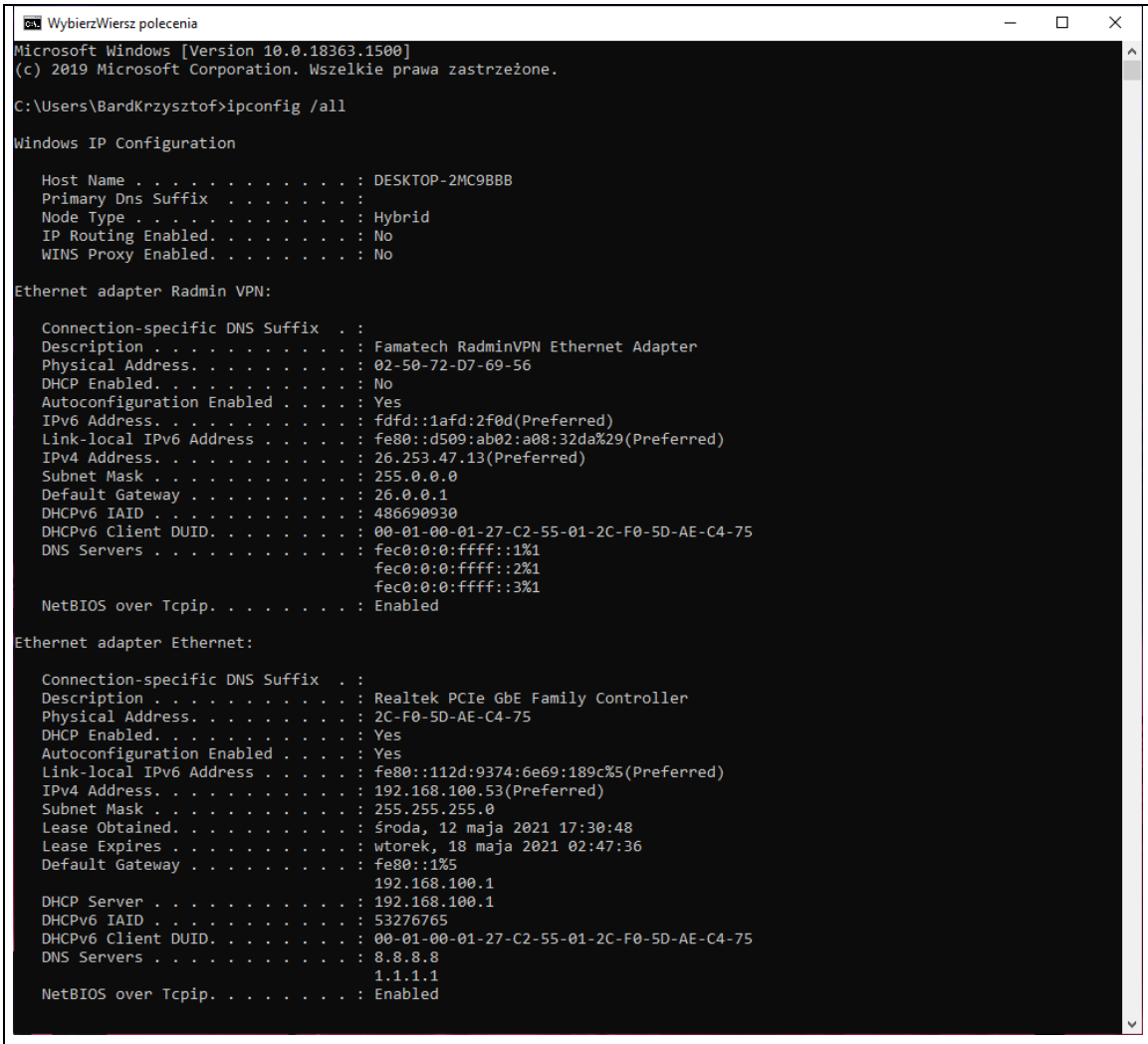


Fig. 3. Initial configuration of computers

As you can see, the gateway addresses are completely different, so computers do not have a physical or logical connection to each other. To create a channel, install RadminVPN on both computers. On one of them you need to start by creating your own network.

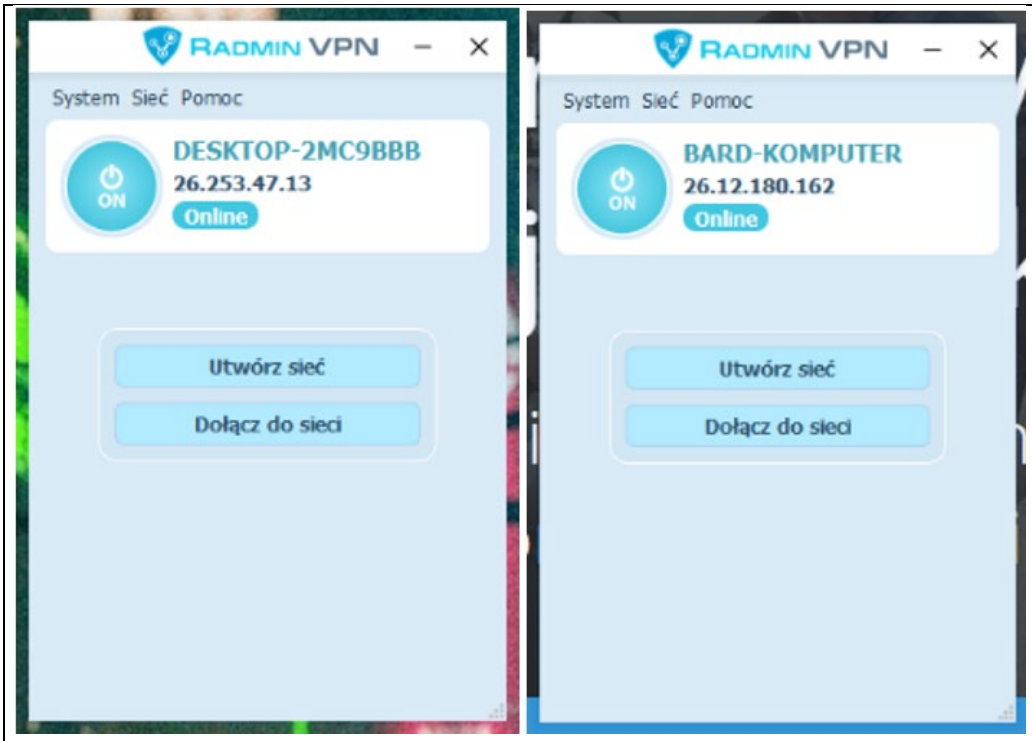


Fig. 4. View of application main screen (left image - configuration of computer 1, right image - computer 2).

To create a network, select **Create network** in the application window, provide a name and password for the network and confirm with the Create button. On the second computer, the network created in this way should be added by clicking the Join the network button, entering the name and password of the network just created.

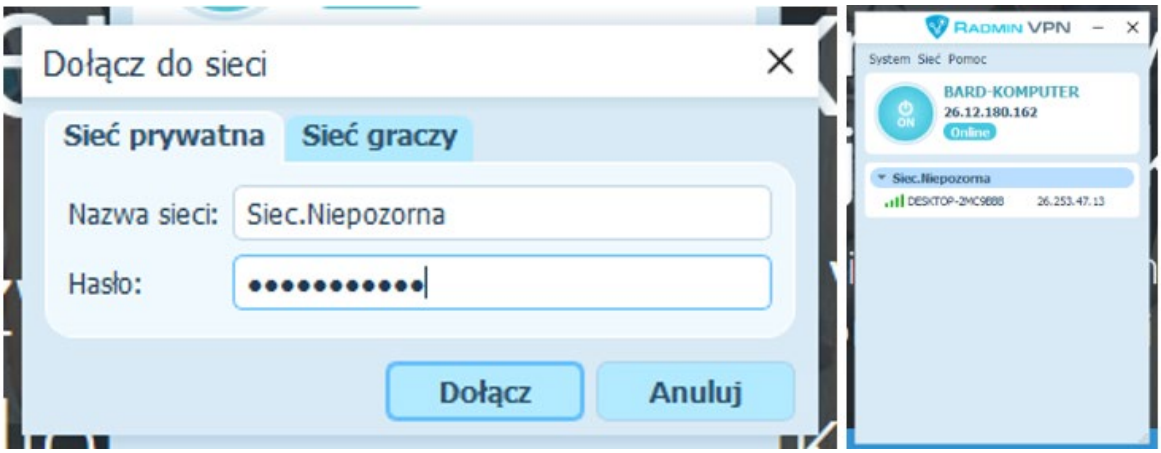


Fig. 5. a) View of the network connection window; b) connection status.

After successfully joining the network, both computers should be in a network connection view (as shown in Figure 5b). In this case, you can see the name and address of the computer on the other

side of the tunnel. It will be the same on the second computer. The connection attempt at this stage will fail as Radmin Server is required for system operation. Information about the installation will appear in the application and it must be done on both computers and restarted. After completing the entire installation process, computers will be able to communicate, but it will not be possible for one to take control over the other. In order to be able to control each other you have to configure the system remote desktop in Windows (Control Panel->System and on the right side choose Advanced System Settings).

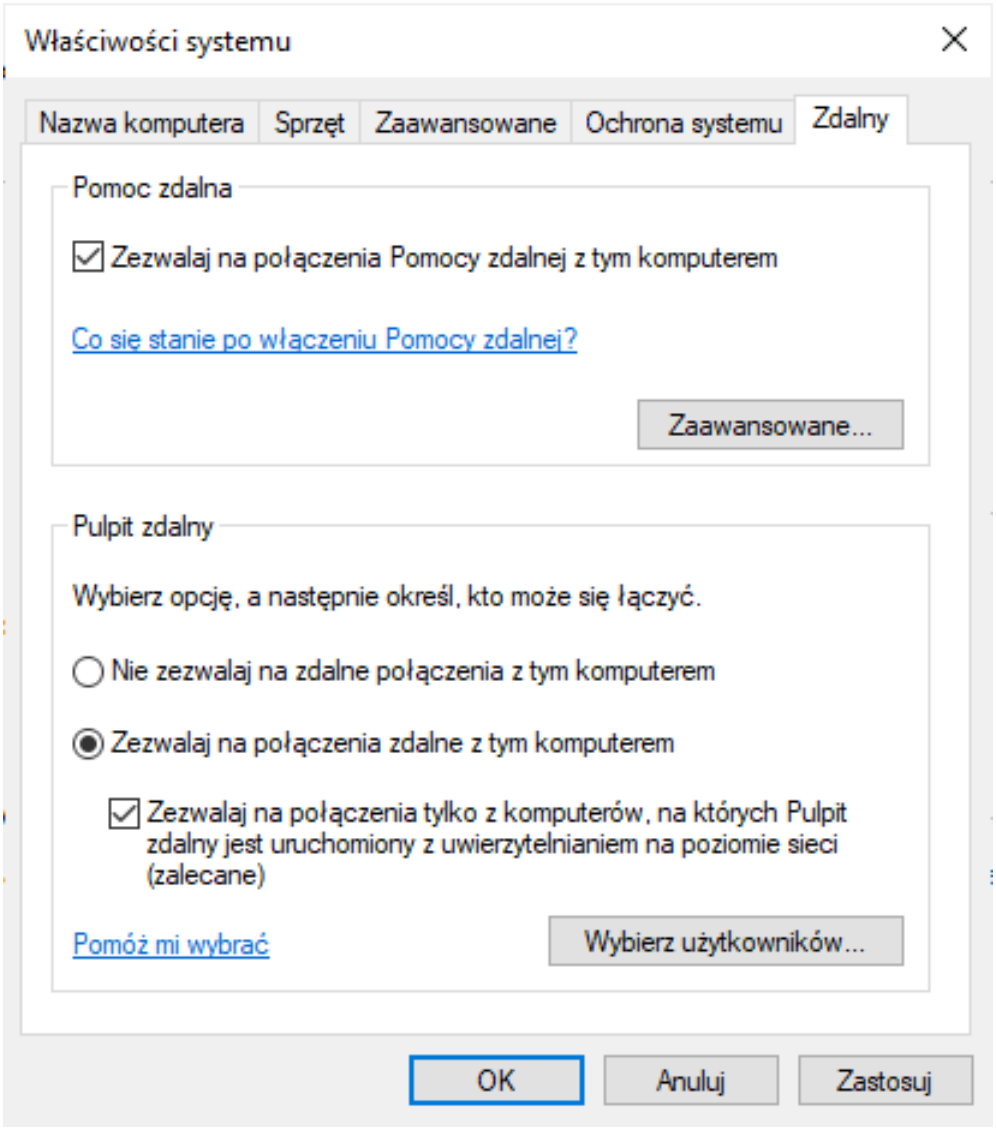


Fig. 6. Settings of Remote Desktop section

The System Properties window appears. Next select the Remote tab and the Remote Desktop section by selecting Allow remote connections to this computer (Fig. 6). After approving the changes on both computers, create a user with given access rights. To do this, run RadminServer

and from the fields on the right choose Permissions and then the Permissions option. In the permissions window, check Full access and create a user (you need to give him/her a name and a password). This completes the VPN channel configuration process. The created tunnel is bi-directional and can be easily used to control computers from both sides.

3. Email encryption. Theoretical basis: types of encryption (symmetric and asymmetric), security, protocols, keys. Installation and configuration of OpenPGP. Installation and configuration of an email client.

One of the most widely used communication channels is electronic mail (email), which is increasingly becoming a target for hacking attacks. Protecting this element is an important part of a cyber security solution package. Protecting email and encrypting attachments are two very important online security issues. Email encryption not only minimizes the risk of confidential data leaking, but prevents unauthorized interception. Email and its attachments are not secured by default with SSL and TLS protocols, and all messages are sent as plain text [8].

Encryption algorithms, like cryptography, fall into two categories:

- symmetric encryption algorithms;
- asymmetric encryption algorithms;

The main difference between the two encryption methods is the number of keys used. Symmetric encryption uses a single key, while asymmetric encryption uses two different but related keys. One of the keys is the private key and the other is the public key. Symmetric encryption algorithms use the same key to perform both encryption and decryption functions. The asymmetric encryption algorithm uses one key to encrypt data and another key to decrypt it. This means that if we want to send an encrypted message to someone, we encrypt it with the recipient's public key, and the recipient uses his/her private key to decrypt it.

Another criterion for dividing encryption is that of key length. The length of the key is directly related to the level of security provided by each of the cryptographic algorithms. The longer the key, the safer the data. In symmetric algorithms, the keys are randomly selected and their length is typically 128 or 256 bits, depending on the level of security required. In the case of asymmetric encryption, in order for encryption and decryption to take place, there must be a mathematical relationship between the public and private keys (in the form of some unique mathematical formula).

Due to its greater speed, symmetric encryption is widely used to protect information in many modern computer systems, such as the Advanced Encryption Standard (AES) used by the US government to encrypt confidential and secret information. AES has replaced the earlier data encryption standard (DES).

Asymmetric encryption is used in systems where multiple users may require access to both encrypt and decrypt a message or data set. An example would be email encryption where the public key can be used to encrypt the message and the private key can be used to decrypt it.

One solution is the OpenPGP standard. Defines cryptographic email extensions - encryption and digital signatures. The standard was based on the existing PGP programme. Currently, there are many different implementations. The standard is defined in RFC 4880. Often, users use the Thunderbird email client in the process of sending emails. This client allows you to send and receive encrypted and digitally signed emails using the OpenPGP standard. This feature is commonly known as end-to-end (e2ee) encryption and makes communication more secure and less likely to be spied on by third parties. Thunderbird 78 has built-in support for two encryption standards, OpenPGP and S/MIME.

Previous versions of Thunderbird (v68 and earlier) had built-in S/MIME support, and you could add OpenPGP support using the Enigmail add-on and GnuPG software. The Enigmail add-on is no longer available for Thunderbird 78, except to help its former users migrate to OpenPGP in Thunderbird 78 or to get guidance on how to restore their 'Junior Mode' rules from Enigmail. You can upgrade your Thunderbird settings from an older version (e.g. 68.x) to version 78.x. Before using Thunderbird 78 for the first time, however, it is recommended that you back up your Thunderbird profile, as after the upgrade, the profile can no longer be used with Thunderbird 68.

Enigmail used GnuPG to store and manage all keys and trusted settings. You can migrate and Enigmail will read the old keys from GnuPG and import them. Thunderbird 78 uses different settings than Enigmail. With Enigmail, it was possible to enable OpenPGP for an email account, but let it automatically choose which key to use. Thunderbird 78 combines these settings. To enable OpenPGP for an email account, you must explicitly specify which key to use.

GPG4win software will be used for encryption. It is a set of advanced data encryption tools. It enables protection against unauthorised access not only of email, but also of files and folders. Working with Gpg4win is based on asymmetric encryption, i.e. on the basis of two keys - private and public. The first one is used to encrypt data, the second one should reach the recipients of the message who can access it. Keep the private key in a safe place.

The package includes such elements as the GnuPG encryption tool, Kleopatra certificate manager (Fig. 7), alternative GPA certificate manager, Claws Mail email client, as well as two plugins that allow integration with Microsoft Outlook (in versions 2003, 2007, 2010 and 2013) and Windows Explorer.

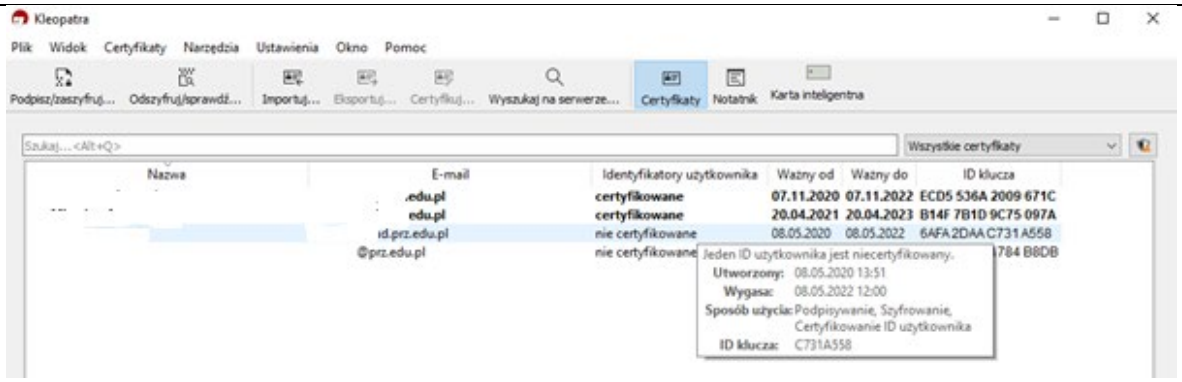


Fig. 7. Certificate manager - Kleopatra.

Gpg4win supports the OpenPGP and S/MIME (X.509) standards, creating certificates by default using 2048-bit keys. RSA is the standard encryption and signing algorithm. Additionally, the package also allows the generation and verification of SHA1, SHA256 and MD5 checksums.

Configuration of the message encryption environment.

After assigning email accounts to the GPG4WIN programme, a pair of keys should be generated. A pair of keys consists of a private key and a public key. The private key is assigned to a specific account. A person who wants to send an encrypted message to this account must have the recipient's public key.

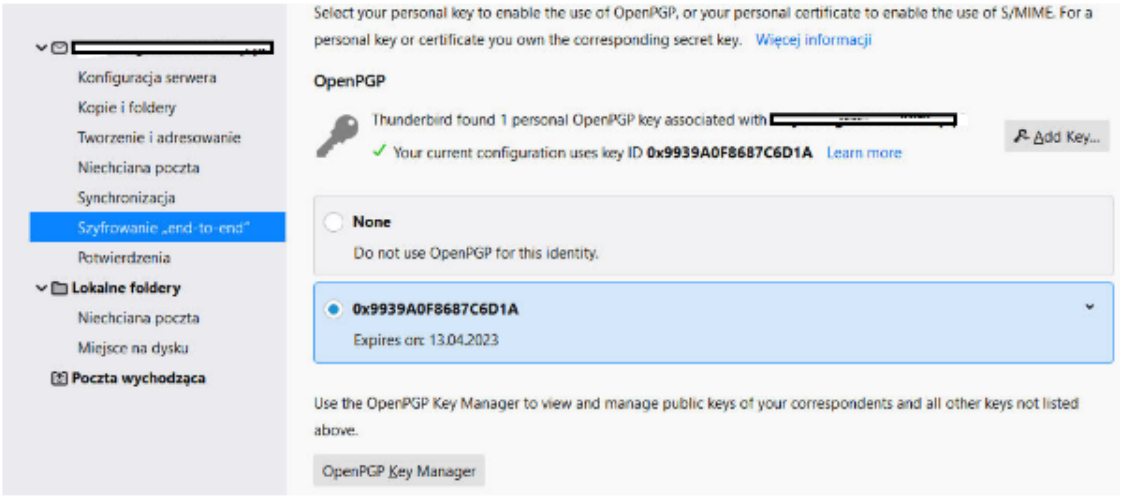
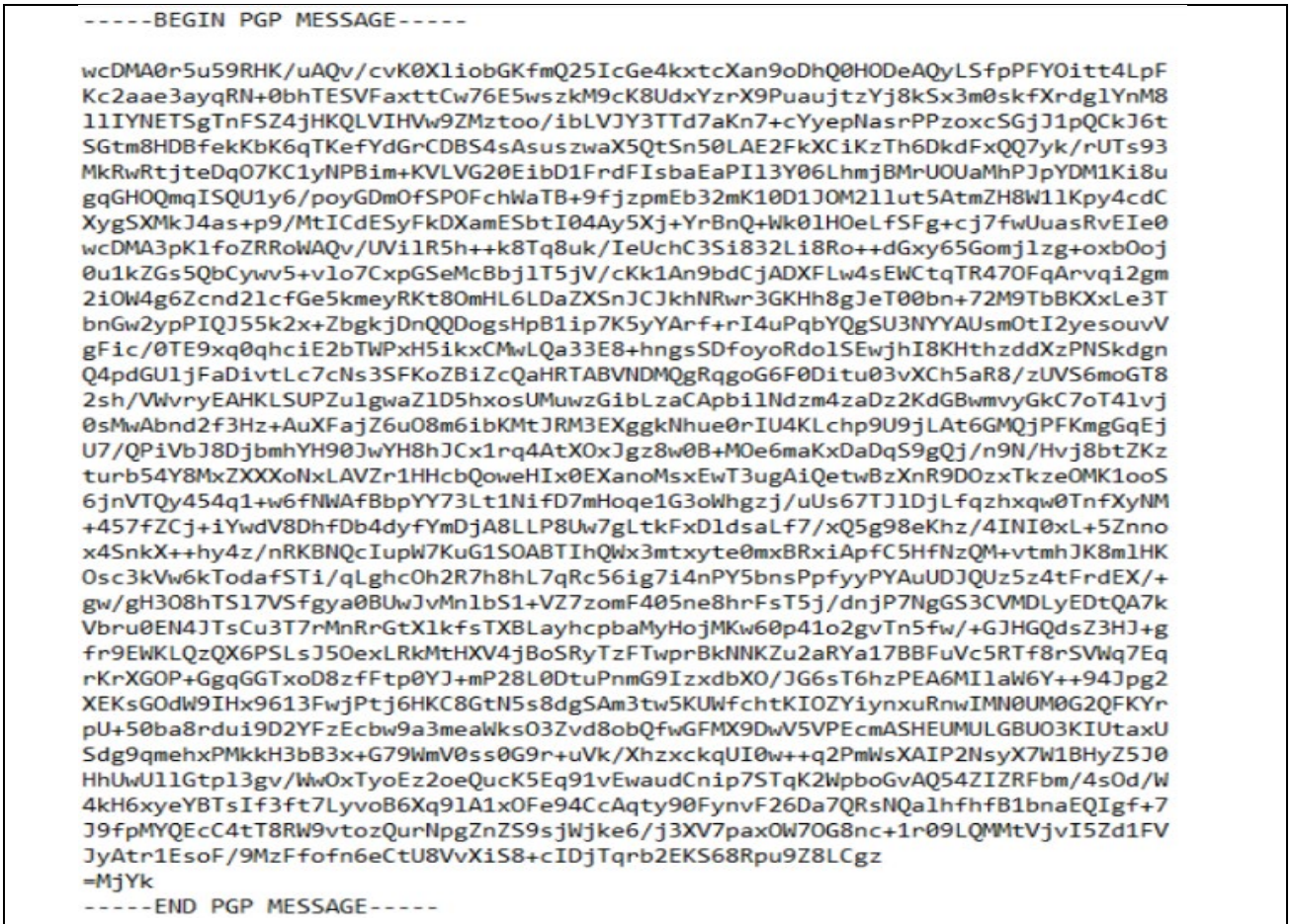


Fig. 8. Settings of Remote Desktop section

Once the accounts have been configured in Cleopatra, you can directly use Thunderbird to send and receive encrypted messages without using an external programme. Remember to send your public key when sending your first message to a new recipient (Fig. 8). An example of an encrypted message is shown in Fig. 9.



```
-----BEGIN PGP MESSAGE-----

wcDMA0r5u59RHK/uAQv/cvK0XliobGKfmQ25IcGe4kxtcXan9oDhQ0HODeAQyLSfpPFYOitt4LpF
Kc2aae3ayqRN+0bhTESVFaxttCw76E5wszkM9cK8UdxYzrX9PuaujtzYj8kSx3m0skfXrdglYnM8
llIYNETSgTnFSZ4jHKQLVIHVw9ZMztoo/ibLVJY3TTd7aKn7+cYyepNasrPPzoxcSGjJ1pQCkJ6t
SGtm8HDBfekKbK6qTKefYdGrCDBS4sAsuszwaX5QtSn50LAE2FkXCiKzTh6DkdFxQQ7yk/rUTs93
MkRwRtjteDqO7KC1yNPBim+KVLVG20EibD1FrdFIsbaEaPIl3Y06LhmjBMrUOUaMhPJpYDM1Ki8u
gqGHOQmqISQU1y6/poyGDmOfSPOFchWaTB+9fjzpmEb32mK10D1JOM2llut5AtmZH8W1lKpy4cdC
XygSXMkJ4as+p9/MtICdESyFkDXamESbtI04Ay5Xj+YrBnQ+Wk0lHOeLfSFg+cj7fwUuasRvEIe0
wcDMA3pKlfoZRRoWAQv/UVilR5h++k8Tq8uk/IeUchC3Si832Li8Ro++dGxy65Gomjlzg+oxbOoj
0u1kZGs5QbCywv5+vlo7CxpGSeMcBbj1T5jV/cKk1An9bdCjADXFLw4sEWCtqTR47OFqArvqi2gm
2iOW4g6Zcnd2lcfGe5kmeyRKt8OmHL6LDaZXSnJCJkhNRwr3GKHh8gJeT00bn+72M9TbBKXxLe3T
bnGw2ypPIQJ55k2x+ZbgkjDnQQDogsHpB1ip7K5yYArf+rI4uPqbYQgSU3NYYAUsmOtI2yesouvV
gFic/0TE9xq0qhciE2bTWPxH5ikxCMwLQa33E8+hngsSDfoyoRdolSEwjhI8KHthzddXzPNSkdgn
Q4pdGU1jFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/zUVS6moGT8
2sh/VWvryEAHKLSUPZulgwaZlD5hxosUMuwzGibLzaCApbilNdzm4zaDz2KdGBwmvyGkC7oT4lvj
0sMwAbnd2f3Hz+AuXFajZ6uO8m6ibKMtJRM3EXggkNhue0rIU4KLchp9U9jLAt6GMQjPFKmgGqEj
U7/QPiVbJ8DjbmhYH90JwYH8hJCx1rq4AtXOxJgz8w0B+MOe6maKxDaDqS9gQj/n9N/Hvj8btZKz
turb54Y8MxZXXXoNxLAVZr1HHcbQoweHIx0EXanoMsxEwT3ugAiQetwBzXnR9DOzxTkzeOMK1ooS
6jnVTQy454q1+w6fNWAfBbpYY73Lt1NifD7mHoqe1G3oWhgzj/uUs67TJlDjLfqzhxqw0TnfXyNM
+457fZCj+iYwdV8DhfDb4dyfYmDjA8LLP8Uw7gLtkFxDldsaLf7/xQ5g98eKhz/4INI0xL+5Znno
x4SnkX++hy4z/nRKBNQcIupW7KuG1SOABTIhQWx3mtxyte0mxBRxiApfC5HfNzQM+vtmhJK8mlHK
Osc3kVw6kTodafSTi/qLghcOh2R7h8hL7qRc56ig7i4nPY5bnsPpfyyPYAuUDJQUz5z4tFrdEX/+
gw/gH3O8hTS17VSfgya0BUwJvMnlbS1+VZ7zomF405ne8hrFsT5j/dnjP7NgGS3CVMDLyEDtQA7k
Vbru0EN4JTsCu3T7rMnRrGtX1kfsTXBLayhcpbaMyHojMKw60p41o2gvTn5fw/+GJHGQdsZ3HJ+g
fr9EWKLQzQX6PSLsJ5OexLRkMtHXV4jBoSRyTzFTwprBkNNKZu2aRYa17BBFuVc5RTf8rSVWq7Eq
rKrXGOP+GgqGGTxoD8zfFtp0YJ+mP28L0DtuPnmG9IzxdbXO/JG6sT6hzPEA6MIlaW6Y++94Jpg2
XEKsGOdW9IHx9613FwjPtj6HKC8GtN5s8dgSAm3tw5KUWfchtKIOZYiynxuRnwIMN0UM0G2QFKYr
pU+50ba8rdui9D2YFzEcbw9a3meaWksO3Zvd8obQfwGFMX9DwV5VPEcmASHEUMULGBUO3KIUtaxU
Sdg9qmehxPMkkH3bB3x+G79WmV0ss0G9r+uVk/XhzxckqUI0w++q2PmWsXAIP2NsyX7W1BHyZ5J0
HhUwU1lGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq9lA1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```

Fig. 9. An example of an encrypted message.

Thunderbird automatically decrypts messages and attachments sent with them. Remember that you need to know the recipients' public keys before sending encrypted correspondence. Encryption with the GPG add-on protects not only the content, but also the attachments. Without knowing the recipient's key, we are unable to send an encrypted message. Additionally, Thunderbird allows you to synchronize several e-mail accounts.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. What is a VPN?
2. How you can use VPN solution?
3. Can you send someone your private key for PGP e-mail encryption?

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

1. Method of secure access to your data from remote access
2. Methods of securing your e-mail conversation

Attachments:

1. Presentation
2. Video movies

References:

1. Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam. (2021). Common Security Protocols for Wireless Networks: A Comparative Analysis. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.
3. Kumkar, Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne, Seema. (2012). Vulnerabilities of Wireless Security protocols (WEP and WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.
4. Costa, Luís & Fdida, Serge & M. B. Duarte, Otto Carlos. (2000). An Introduction to Virtual Private Networks: Towards D-VPNs.
5. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/
6. https://www.radmin-vpn.com
7. https://www.fortinet.com/resources/cyberglossary/pgp-encryption