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

InCyT træningsmoduler

Informationssikkerhed for medarbejdere **Enhed nr: (3) Uge 5** **Navn på enhed (modul): (Sikkerhed ved forretningsrejser)**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑ **Andet**
Læringsansvarlig	• Mirosław Mazurek • Paweł Dymora
Læringsaktivitetsmål	1. Trådløse netværk 2. VPN 3. Email kryptering
Færdigheder, der skal opnås	• **TS3** • **SS2**
Varighed af læringsaktivitet	2 uger
Læring krav	***Hvad skal der til?***
	• Internetadgang • Internet browser • MS Office365

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

Kort information om modulet

Beskrivelse
Den generelle oversigt over dette modul er at give nogle teoretiske og praktiske spørgsmål relateret til viden og praktiske færdigheder sikkerhed på forretningsrejser. Du vil have mulighed for at beskytte dit trådløse netværk og bruge beskyttede trådløse netværk med ideen om VPN. Modulet vil også dække, hvordan man sender e-mails sikkert ved hjælp af gratis PGP-protokol til krypterede meddelelser, som ingen kan dechifrere uden din tilladelse.

Lærematerialets indhold

1. Introduktion til trådløse netværk. Teoretisk grundlæggende: funktionsprincip, krypteringsprotokoller.

Tidligere WEP- og WPA-protokoller blev brugt til at sikre trådløse netværk, men de var ikke modstandsdygtige over for hackers angreb. Introduktionen af WPA2-protokollen gjorde det muligt at sikre et tilstrækkeligt sikkerhedsniveau, men den giver alligevel ikke fuld sikkerhed. Der er mange netværkstopologier, trådløse adgangsprotokoller og teknikker til erhvervelse af netværksadgang tilgængelige, og både CPU (Central Processing Unit) og GPU (Graphics Processing Unit) computerarkitekturer bruges i netværksnøgleopsamling [1,2].

WEP (Wired Equivalent Privacy) er en af de ældste IEEE 802.11 trådløse krypteringsstandarder. Det giver informationsbeskyttelse baseret på brugen af RC4-algoritmen. Den har mange kendte sikkerhedssårbarheder og er derfor blevet knækket flere gange. Det er en af de ældste standarder for sikring af WLAN-netværk (etableret i 1997). Det kræver ikke høj computerkraft af de installerede enheder. Den bruger to brugergodkendelsesmetoder: Åben godkendelse og delt nøglegodkendelse. Derudover muliggør den brugerverifikation baseret på fysiske MAC-adresser ved hjælp af ACL (Access Control List). Der er en 64-bit WEP-variant (baseret på en 40-bit nøgle og 24-bit initialiseringsvektor) og en 128-bit WEP-variant (baseret på en 104-bit nøgle). Nogle producenter har også introduceret en 256-bit WEP-standard [1,2].

WPA (Wi-Fi Protected Access) er en anden standard for kryptering af IEEE 802.11 trådløse netværk. Det blev introduceret for at forbedre sikkerhedsniveauet for WLAN-netværk og erstatte kendte sårbarheder i WEP-standarden. Den er baseret på brugen af protokoller: TKIP (Temporal Key Integrity Protocol) og EAP (Extensible Authentication Protocol), 802.1x-standarden og MIC-mekanismen (Message Integrity Check). Standarden er baseret på RC4-algoritmen. Det blev implementeret som en midlertidig løsning mellem WEP-standarden og den nuværende mest sikre

trådløse krypteringsstandard 802.11i. Det giver arbejde i to tilstande, som inkluderer: Enterprise (ved hjælp af en RADIUS-server, der styrer tildelingen af nøgler til brugere) og Personal (ved hjælp af en delt PSK-nøgle) [1,2].

WPA2 (Wi-Fi Protected Access 2) er i øjeblikket den mest kraftfulde krypteringsstandard for trådløse netværk (også kendt som 802.11i). Det giver informationsbeskyttelse baseret på brugen af AES (Advanced Encryption Standard). Det blev introduceret for at forbedre sikkerhedsniveauet for WLAN-netværk og erstatte kendte sårbarheder i WEP-standarden og den midlertidige WPA-standard. Den implementerer 802.1x-protokollen, der forbedrer kontrollen af brugeradgang til netværket. Det giver arbejde i to tilstande, som omfatter: Enterprise (ved hjælp af en RADIUS-server, der styrer tildelingen af nøgler til brugere) og Personal (ved hjælp af en delt PSK-nøgle) - ofte brugt i hjemmeløsninger i dag [1,2].

WEP-algoritmen er den mindst sikre krypteringsstandard for IEEE 802.11 trådløse netværk. Det er blevet knækket mange gange af forskellige metoder på grund af de mange i øjeblikket kendte sårbarheder i sikkerhedsaspekterne af algoritmen. De største ulemper ved standarden omfatter[3]:

- Mangel på et defineret nøglestyringssystem (ofte bruges én netværksnøgle af alle noder i et trådløst netværk);
- Utilstrækkelig bitstørrelse af netværksnøglen (den første version af WEP-standarden introducerer 40-bit nøgler);
- Utilstrækkelig bitstørrelse på IV-initieringsvektoren (WEP-standarden introducerer en 24-bit initialiseringsvektor, som viser sig at være utilstrækkelig, og på grund af den relativt høje sandsynlighed for kollisioner med et lille antal modtagne pakker er der mulighed for et kryptografisk angreb for at opnå værdien af WEP-nøglen);
- Svag ICV-kontrolsum baseret på CRC-32 lineær funktion (der er mulighed for umærkelig ændring af informationen sendt i netværket);
- Svag RC4 informationskrypteringsalgoritme (der er for mange afhængigheder mellem netværksnøglen og resultatet af informationskryptering);
- Utilstrækkeligt brugergodkendelsessystem (der er mulighed for at forfalske godkendelsesmeddelelser).
- Baseret på de præsenterede svagheder ved WEP-algoritmen er der skabt mange værktøjer til at udføre angreb, der tester sikkerhedsniveauet for WLAN-netværk. De mest populære angreb mod WEP inkluderer:
- FMS-angreb - et statistisk angreb (udviklet af Fluhrer, Mantin og Shamir) på RC4-algoritmen brugt i WEP-krypteringsstandarden;
- KoreK-angreb - et statistisk angreb (udviklet af en person med kælenavnet KoreK), der bruger adskillige flere (sammenlignet med FMS-angrebet) afhængigheder af RC4-algoritmens krypteringsprocessen;
- Chopchop- angreb - et interaktivt angreb, udført i retning af at få adgang til netværket ved gradvist at dekryptere en af de modtagne pakker;

- PTW-angreb - er et statistisk angreb (udviklet af Pyshkin , Tews og Weinmann) på RC4-algoritmen, som takket være de successive afhængigheder af datakrypteringsprocessen øger sandsynligheden for at opnå nøgleværdien med et relativt lille antal modtagne pakker.

En anden hyppigt brugt type angreb er ordbogsangrebet. Det er en af brute-force metoderne til at erhverve fx kryptografiske nøgleværdier i trådløse computernetværk. For at opnå WPA/WPA2-nøgleværdier er metoden baseret på envejskryptering og sammenligning af indgange i ordbogen med information i den opfangede 4-vejs håndtryksekvens. Ordbogsangreb udføres med den hensigt at reducere tiden for opnåelse af nøgleværdier sammenlignet med brute-force-metoden. Processen med at hente nøgleværdien fortsætter, indtil der opnås et positivt resultat (dvs. når indtastningen i ordbogen viser sig at være en gyldig nøgleværdi), eller indtil alle indtastninger i ordbogen sammenlignes med det negative resultat. Et negativt resultat kan indikere et højt niveau af kompleksitet af nøgleværdien og behovet for at bruge brute-force-metoden[3].

Succesen med dette angreb er valget af en passende ordbog. Ordbog er en tekstfil, der bruges i tilfælde af ordbogsangreb til at opnå for eksempel kryptografiske nøgleværdier. Den indeholder en liste over passende forberedte elementer, der kan udgøre den søgede nøgleværdi. Brugen af ordbøger i tilfælde af kraftangreb gør det muligt at reducere mængden af undersøgte værdier betydeligt, hvilket kan resultere i at fremskynde processen med at erhverve den kryptografiske nøgleværdi. Indholdet af ordbøger er for eksempel bygget på baggrund af de præsenterede punkter[3]:

- en liste over ord, der optræder i nationale og udenlandske ordbøger;
- kombinationer af ord med store og små bogstaver, ord stavet baglæns (dvs. palindromer);
- kombinationer af ordbogsposter med udskårne vokaler eller konsonanter;
- kombinationer af flere gentagelser af udvalgte navne, efternavne, ordbogsposter;
- kombinationer af ord med numeriske værdier, specialtegn osv.;
- en liste over adgangskoder og logins, der oftest bruges af brugere;
- en liste over populære virksomheder, organisationer, tekniske termer, egennavne osv.;
- informationslækager (dvs. logins, kaldenavne, adgangskoder) fra forskellige internetportaler;
- kombinationer af tilstødende tastaturtegn for udvalgte mønstre (fig. 1).

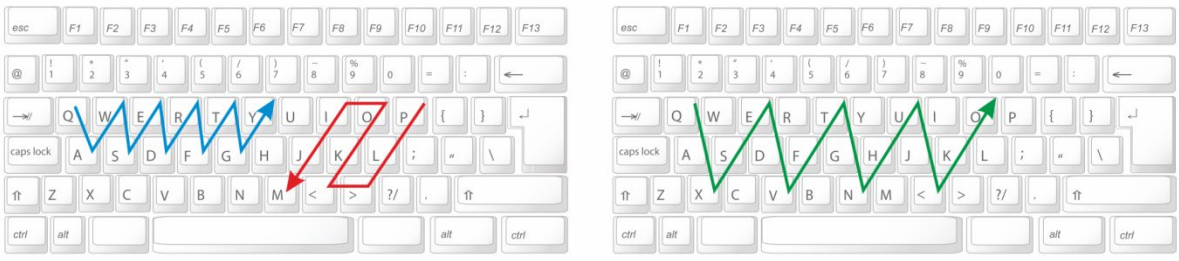


Fig. 1 . Skema, der viser eksempler på mønstre for oprettelse af netværksnøgler

Netværksnøglen spiller en nøglerolle i studiet af netværksresiliens. Det er en sekvens af tegn, der bruges af netværksbrugere i godkendelsesprocessen. Godkendelsesprocessen er et vigtigt skridt i at beskytte adgangen til delte tjenester og netværksressourcer mod uautoriserede brugere. Netværksnøgler oprettes og administreres ofte af netværksadministratorer og kan udgøre det svageste led i et computernetværks sikkerhed. Nøgleværdier, der viser sig at være relativt tidskrævende eller umulige at bryde ved brug af brute-force-metoder i realistisk tid, bør for eksempel genereres baseret på de præsenterede regler [3]:

- Hvert trådløst netværk, der administreres af administratoren, skal sikres med en anden netværksnøgle;
- Hver netværksbruger skal bruge en individuel netværksnøgle;
- Netværksnøgler skal bygges på et tilstrækkeligt antal tegn;
- Genereringen af nøgler bør være baseret på den maksimalt tilgængelige tegnplads;
- Nøgler bør ikke genereres ved hjælp af virksomheds- og personlige oplysninger;
- Generering af nøgler bør ikke være baseret på en liste over emner i offentligt tilgængelige ordbøger;
- Netværksnøgler bør bygges på basis af tilfældige sekvenser af tegn;
- Netværksnøgler bør opdateres med jævne mellemrum;
- Aktuelt anvendte nøgleværdier bør ikke associeres med nøgleværdier, der ikke længere bruges.

2. Virtuelle VPN-tunneler. Teoretisk grundlag: typer, arkitektur, funktionsprincip, krypteringsprotokoller. Installation af Open VPN-programmet (konfiguration, adressering, parametervalg, nøglegenerering).

Et virtuelt privat netværk er en tunnel, hvorigennem privat netværkstrafik flyder mellem afsender og modtager over et offentligt netværk. VPN står for 'Virtual Private Network'. Et VPN-netværk krypterer alle aktiviteter på internettet, skjuler IP-adressen og beskytter netværksbrugerens identitet. En VPN-forbindelse giver sikker adgang til applikationer, websteder og underholdningsplatforme fra hvor som helst i verden. Det er muligt valgfrit at komprimere eller kryptere overførte data for at give bedre kvalitet eller et højere sikkerhedsniveau og dermed beskytte privatlivets fred i netværket [4].

En sikker tunnel oprettes ved først at autentificere klienten med VPN-serveren. Serveren anvender derefter en krypteringsprotokol til alle data, der sendes og modtages. For at sikre sikkerheden af hver datapakke placerer VPN den i en ekstern pakke, som derefter krypteres ved indkapsling. Det sikrer datasikkerheden under transmissionen og er en grundlæggende komponent i VPN-tunnelen. Efter at dataene når serveren, fjernes de eksterne pakker i dekrypteringsprocessen [4] .

VPN'er kan opdeles i to hovedkategorier [5] :

- En fjernadgangs-VPN, der giver brugerne mulighed for at oprette forbindelse til et fjernnetværk, normalt gennem speciel software.
- Site-to-site VPN'er, der bruges af virksomheder, især store virksomheder. De giver brugere på udvalgte steder mulighed for sikker adgang til andre brugeres netværk.

Et eksempel på en dedikeret VPN-udviklingssoftware er *RadminVPN* . I de fleste tilfælde er det ikke nødvendigt at have en statisk IP-adresse i dit lokale netværk for at oprette en VPN-tunnel. Efter at have downloadet den relevante software, vil den oprette et passende netværk med en statisk adresse på din computer [6] .

Radmin VPN giver dig mulighed for at oprette forbindelse til to computere på to forskellige netværk. Et konfigurationseksempel er vist nedenfor. For lettere forståelse af driften af VPN-kanalen viser fig. 2 og 3 den indledende konfiguration af computere, mellem hvilke der skal oprettes en sikker kanal.

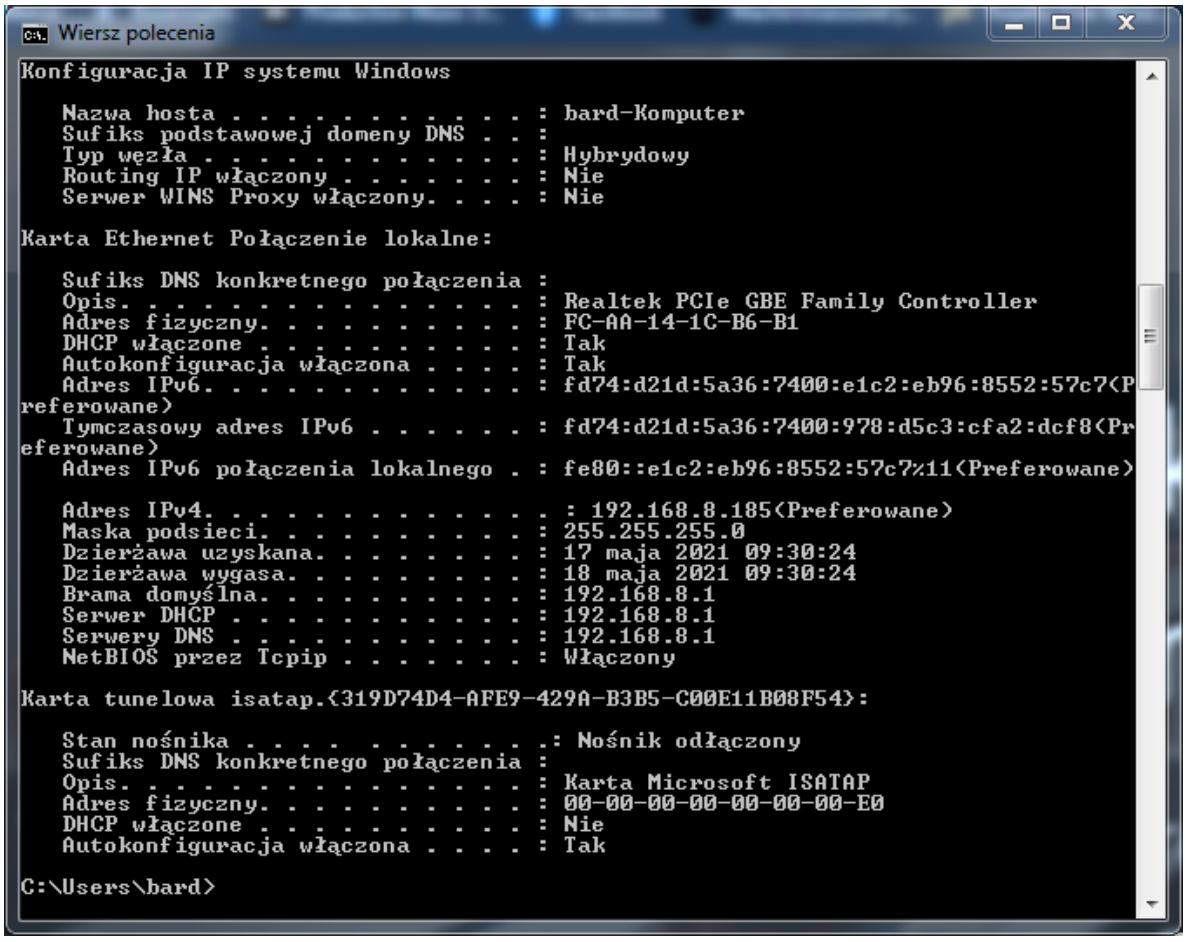


Fig. 2. Indledende konfiguration af computere

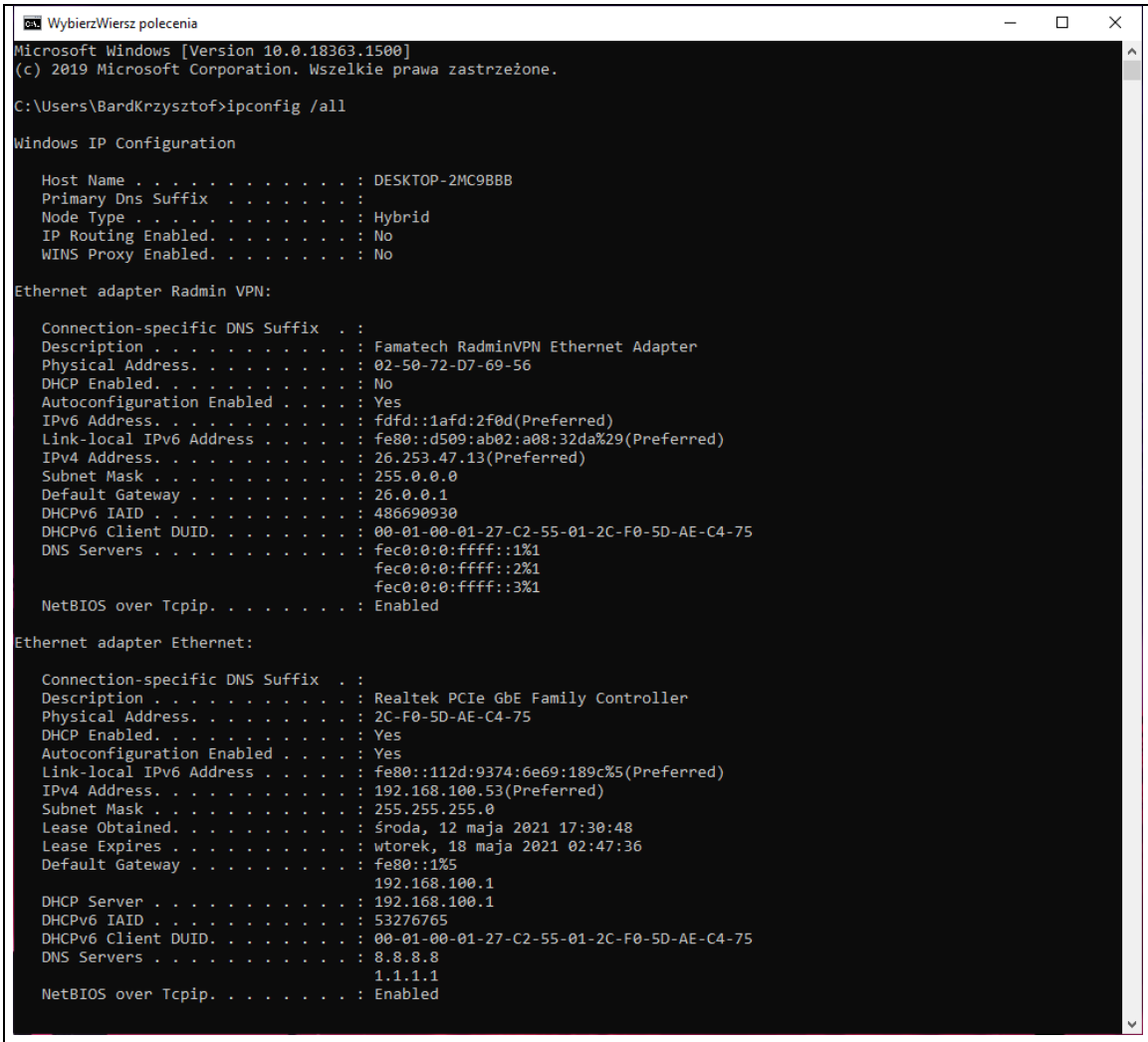


Fig. 3. Indledende konfiguration af computere

Som du kan se, er gateway-adresserne helt forskellige, så computere har ikke en fysisk eller logisk forbindelse til hinanden. For at oprette en kanal skal du installere RadminVPN på begge computere. På en af dem skal du starte med at skabe dit eget netværk.

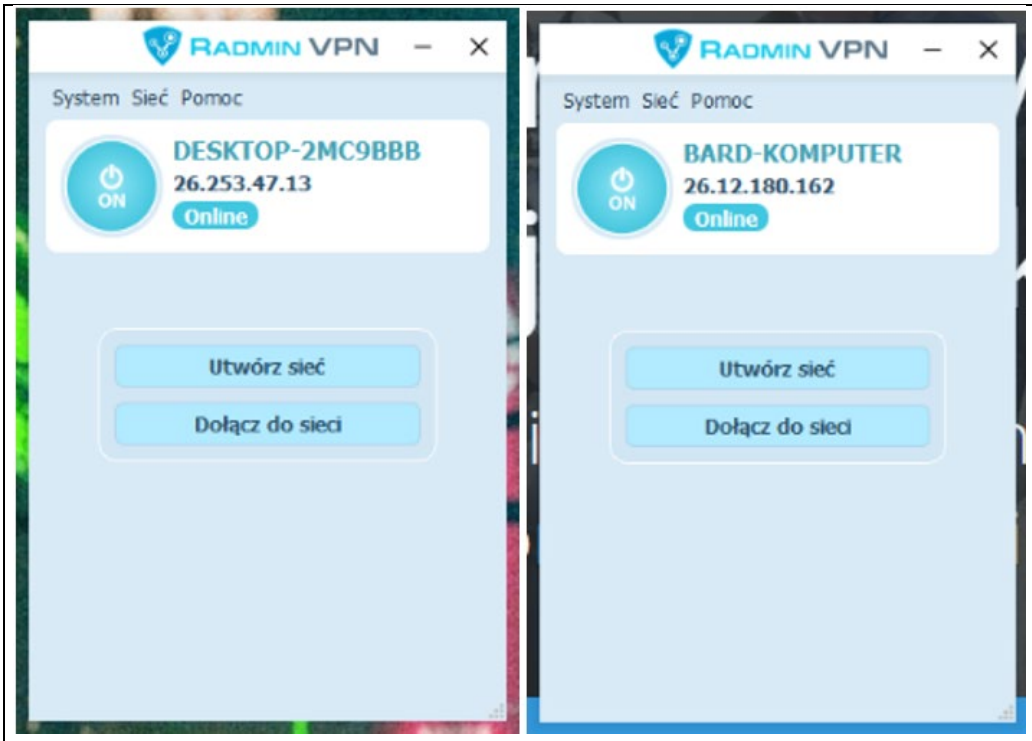


Fig. 4. Visning af applikationens hovedskærm (venstre billede - konfiguration af computer 1, højre billede - computer 2).

For at oprette et netværk skal du vælge **Opret netværk** i programvinduet, angive et navn og en adgangskode til netværket og bekræfte med knappen Opret. På den anden computer skal det netværk, der er oprettet på denne måde, tilføjes ved at klikke på knappen Deltag i netværket og indtaste navnet og adgangskoden til det netværk, der netop er oprettet.

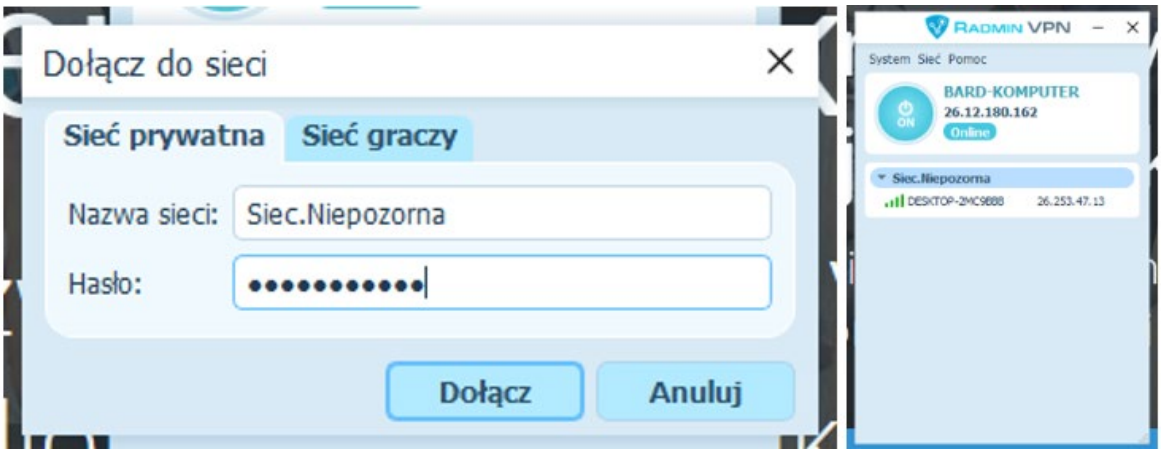


Fig. 5. a) Visning af netværksforbindelsesvinduet; b) forbindelsesstatus.

Når du har tilsluttet netværket, skal begge computere være i en netværksforbindelsesvisning (som vist i figur 5b). I dette tilfælde kan du se navn og adresse på computeren på den anden side af

tunnelen. Det vil være det samme på den anden computer. Tilslutningsforsøget på dette trin vil mislykkes, da Radmin Server er påkrævet til systemdrift. Oplysninger om installationen vil fremgå af applikationen, og det skal ske på begge computere og genstartes. Efter at have fuldført hele installationsprocessen, vil computere være i stand til at kommunikere, men det vil ikke være muligt for den ene at tage kontrol over den anden. For at kunne styre hinanden skal du konfigurere systemets fjernskrivebord i Windows (Kontrolpanel->System og i højre side vælge Avancerede systemindstillinger).

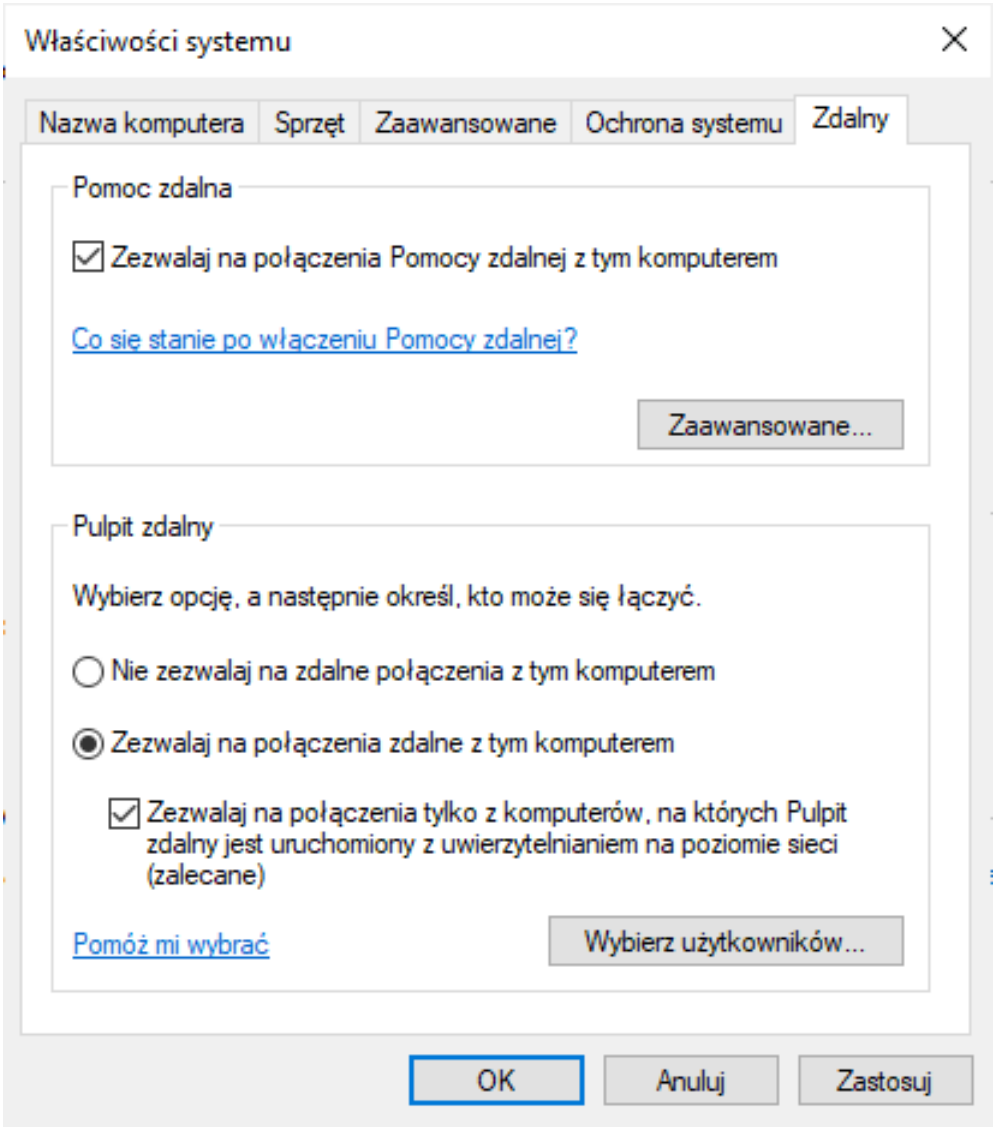


Fig. 6. Indstillinger for Fjernskrivebord sektion

Vinduet Systemegenskaber vises. Vælg derefter fanen Remote og sektionen Remote Desktop ved at vælge Tillad fjernforbindelser til denne computer (fig. 6). Efter at have godkendt ændringerne på begge computere, skal du oprette en bruger med givne adgangsrettigheder. For at gøre dette skal

du køre RadminServer og fra felterne til højre skal du vælge Tilladelser og derefter indstillingen Tilladelser. I tilladelsesvinduet skal du markere Fuld adgang og oprette en bruger (du skal give ham/hende et navn og en adgangskode). Dette fuldender VPN-kanalkonfigurationsprocessen. Den oprettede tunnel er tovejsbestemt og kan nemt bruges til at styre computere fra begge sider.

3. Email kryptering. Teoretisk grundlag: typer af kryptering (symmetrisk og asymmetrisk), sikkerhed, protokoller, nøgler. Installation og konfiguration af OpenPGP. Installation og konfiguration af en e-mail-klient.

En af de mest brugte kommunikationskanaler er elektronisk post (e-mail), som i stigende grad bliver et mål for hackingangreb. Beskyttelse af dette element er en vigtig del af en cybersikkerhedsløsningspakke. Beskyttelse af e-mail og kryptering af vedhæftede filer er to meget vigtige online sikkerhedsproblemer. E-mail-kryptering minimerer ikke kun risikoen for, at fortrolige data lækker, men forhindrer uautoriseret aflytning. E-mail og dens vedhæftede filer er ikke sikret som standard med SSL- og TLS-protokoller, og alle meddelelser sendes som almindelig tekst [8] .

Krypteringsalgoritmer, ligesom kryptografi, falder i to kategorier:

- symmetriske krypteringsalgoritmer;
- asymmetriske krypteringsalgoritmer;

Den største forskel mellem de to krypteringsmetoder er antallet af anvendte nøgler. Symmetrisk kryptering bruger en enkelt nøgle, mens asymmetrisk kryptering bruger to forskellige, men relaterede nøgler. En af nøglerne er den private nøgle, og den anden er den offentlige nøgle. Symmetriske krypteringsalgoritmer bruger den samme nøgle til at udføre både krypterings- og dekrypteringsfunktioner. Den asymmetriske krypteringsalgoritme bruger én nøgle til at kryptere data og en anden nøgle til at dekryptere dem. Det betyder, at hvis vi ønsker at sende en krypteret besked til nogen, krypterer vi den med modtagerens offentlige nøgle, og modtageren bruger sin private nøgle til at dekryptere den.

Et andet kriterium for opdeling af kryptering er nøglelængden. Nøglens længde er direkte relateret til det sikkerhedsniveau, der leveres af hver af de kryptografiske algoritmer. Jo længere nøglen er, jo sikrere data. I symmetriske algoritmer er nøglerne tilfældigt udvalgt, og deres længde er typisk 128 eller 256 bit, afhængigt af det nødvendige sikkerhedsniveau. Ved asymmetrisk kryptering skal der, for at kryptering og dekryptering kan finde sted, være et matematisk forhold mellem de offentlige og private nøgler (i form af en eller anden unik matematisk formel).

På grund af dens højere hastighed er symmetrisk kryptering i vid udstrækning brugt til at beskytte information i mange moderne computersystemer, såsom Advanced Encryption Standard (AES), der bruges af den amerikanske regering til at kryptere fortrolige og hemmelige oplysninger. AES har erstattet den tidligere datakrypteringsstandard (DES).

Asymmetrisk kryptering bruges i systemer, hvor flere brugere kan kræve adgang til både at kryptere og dekryptere en besked eller et datasæt. Et eksempel ville være e-mail-kryptering, hvor

den offentlige nøgle kan bruges til at kryptere beskeden, og den private nøgle kan bruges til at dekryptere den.

En løsning er OpenPGP-standarden. Definerer kryptografiske e-mail-udvidelser - kryptering og digitale signaturer. Standarden var baseret på det eksisterende PGP -program . I øjeblikket er der mange forskellige implementeringer. Standarden er defineret i RFC 4880. Ofte bruger brugere Thunderbird e-mail-klienten i processen med at sende e-mails. Denne klient giver dig mulighed for at sende og modtage krypterede og digitalt signerede e-mails ved hjælp af OpenPGP-standarden. Denne funktion er almindeligvis kendt som end-to-end (e2ee) kryptering og gør kommunikation mere sikker og mindre tilbøjelig til at blive spioneret af tredjeparter. Thunderbird 78 har indbygget understøttelse af to krypteringsstandarder, OpenPGP og S/MIME.

Tidligere versioner af Thunderbird (v68 og tidligere) havde indbygget S/MIME-understøttelse, og du kunne tilføje OpenPGP-understøttelse ved hjælp af Enigmail -tilføjelsen og GnuPG-softwaren. Enigmail - tilføjelsen er ikke længere tilgængelig for Thunderbird 78, undtagen for at hjælpe dets tidligere brugere med at migrere til OpenPGP i Thunderbird 78 eller for at få vejledning i, hvordan man gendanner deres 'Junior Mode'-regler fra Enigmail . Du kan opgradere dine Thunderbird-indstillinger fra en ældre version (f.eks. 68.x) til version 78.x. Før du bruger Thunderbird 78 for første gang, anbefales det dog, at du sikkerhedskopierer din Thunderbird-profil, da profilen efter opgraderingen ikke længere kan bruges med Thunderbird 68.

Enigmail brugte GnuPG til at gemme og administrere alle nøgler og betroede indstillinger. Du kan migrere, og Enigmail vil læse de gamle nøgler fra GnuPG og importere dem. Thunderbird 78 bruger andre indstillinger end Enigmail . Med Enigmail var det muligt at aktivere OpenPGP for en e-mail-konto, men lade den automatisk vælge, hvilken nøgle der skulle bruges. Thunderbird 78 kombinerer disse indstillinger. For at aktivere OpenPGP for en e-mail-konto skal du udtrykkeligt angive, hvilken nøgle der skal bruges.

GPG4win software vil blive brugt til kryptering. Det er et sæt avancerede datakrypteringsværktøjer. Det muliggør beskyttelse mod uautoriseret adgang, ikke kun til e-mail, men også til filer og mapper. Arbejdet med Gpg4win er baseret på asymmetrisk kryptering, altså på basis af to nøgler - private og offentlige. Den første bruges til at kryptere data, den anden skal nå frem til modtagerne af beskeden, som kan få adgang til den. Opbevar den private nøgle et sikkert sted.

Pakken indeholder elementer som GnuPG-krypteringsværktøjet, Kleopatra-certifikathåndtering (fig. 7), alternativ GPA-certifikathåndtering, Claws Mail-e-mail-klient, samt to plugins, der tillader integration med Microsoft Outlook (i version 2003, 2007, 2010 og 2013) og Windows Stifinder.

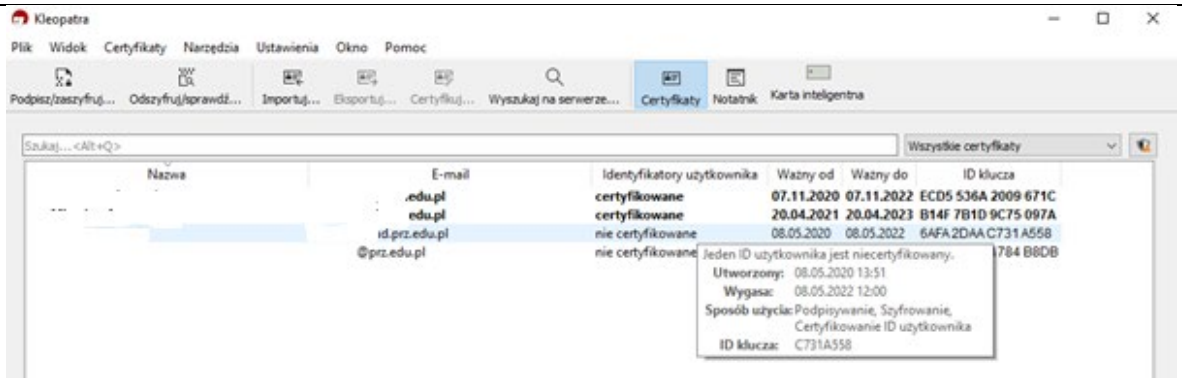


Fig. 7. Certifikatansvarlig - Kleopatra.

Gpg4win understøtter OpenPGP- og S/MIME (X.509)-standarderne, og skaber certifikater som standard ved hjælp af 2048-bit nøgler. RSA er standard krypterings- og signeringsalgoritme. Derudover tillader pakken også generering og verifikation af SHA1, SHA256 og MD5 kontrolsummer.

Konfiguration af meddelelseskrypteringsmiljøet.

Efter at have tildelt e-mail-konti til GPG4WIN- programmet , skal der genereres et par nøgler. Et par nøgler består af en privat nøgle og en offentlig nøgle. Den private nøgle er tildelt en bestemt konto. En person, der ønsker at sende en krypteret besked til denne konto, skal have modtagerens offentlige nøgle.

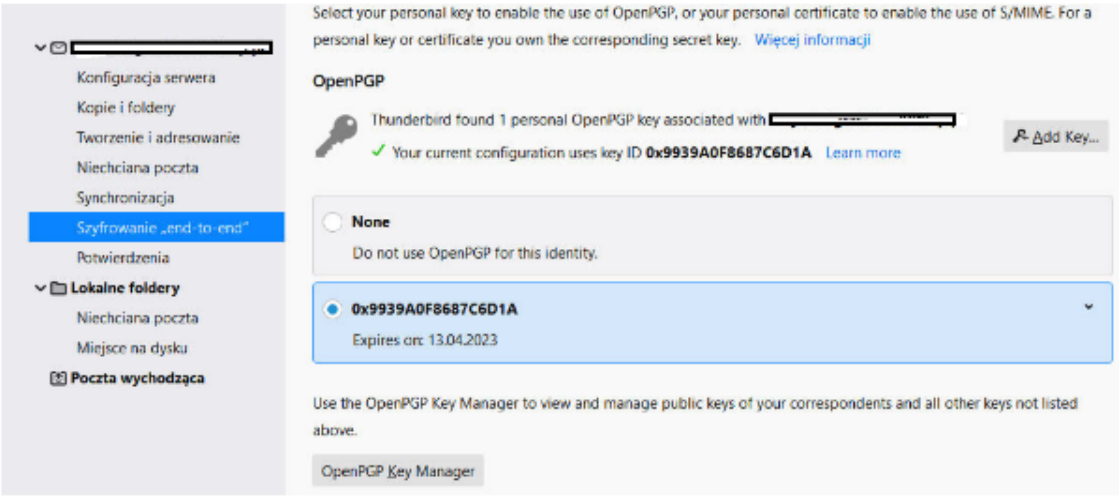
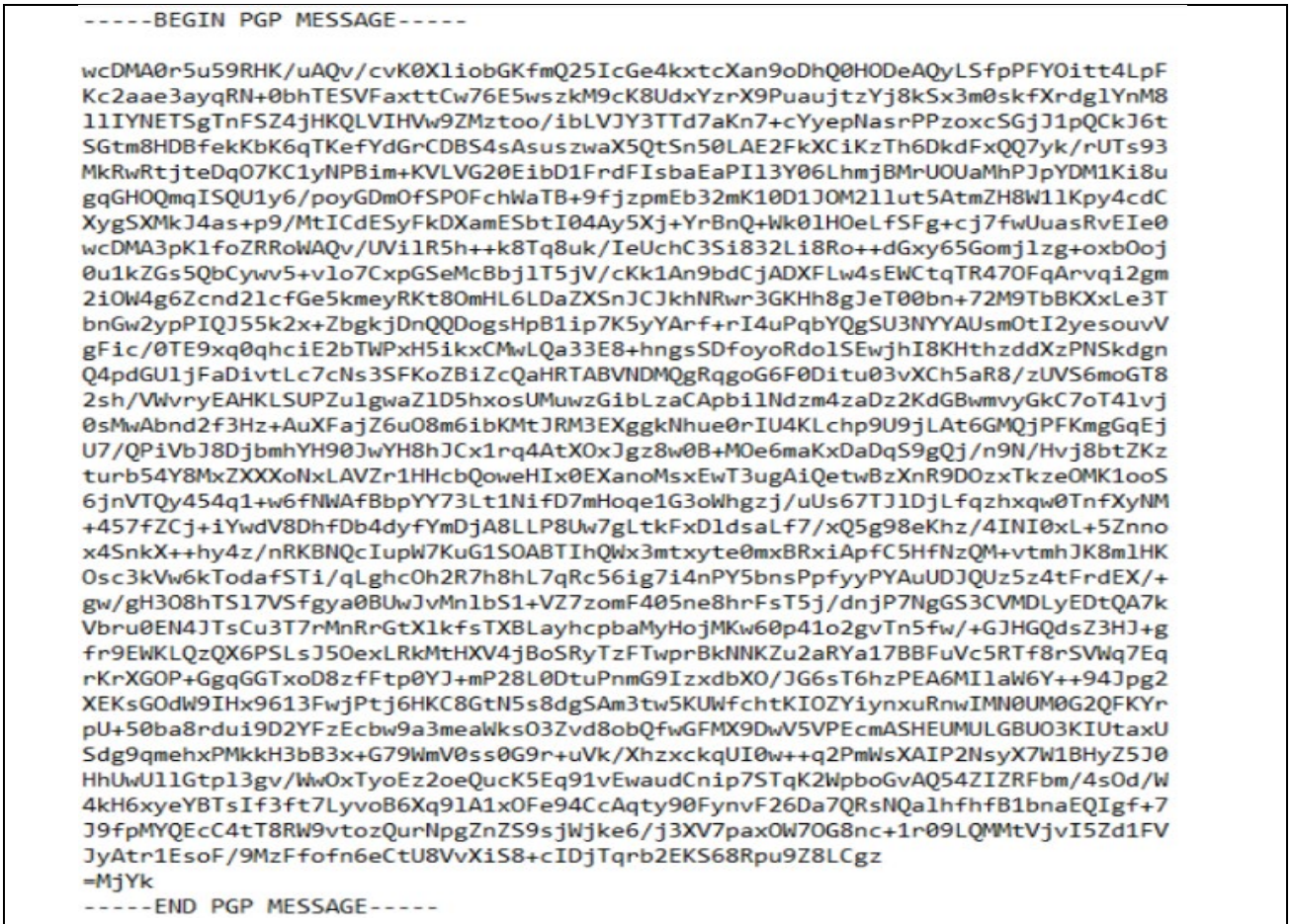


Fig. 8. Indstillinger for Fjernskrivebord sektion

Når konti er blevet konfigureret i Cleopatra, kan du direkte bruge Thunderbird til at sende og modtage krypterede beskeder uden at bruge et eksternt program . Husk at sende din offentlige nøgle, når du sender din første besked til en ny modtager (fig. 8). Et eksempel på en krypteret besked er vist i 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
Q4pdGUljFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/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
HhUwUllGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq9lA1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```

Fig. 9. Et eksempel på en krypteret besked.

Thunderbird dekrypterer automatisk meddelelser og vedhæftede filer, der sendes med dem. Husk, at du skal kende modtagernes offentlige nøgler, før du sender krypteret korrespondance. Kryptering med GPG-tilføjelsen beskytter ikke kun indholdet, men også de vedhæftede filer. Uden at kende modtagerens nøgle, er vi ikke i stand til at sende en krypteret besked. Derudover giver Thunderbird dig mulighed for at synkronisere flere e-mail-konti.

Spørgsmål :

Spørgsmål Diskussionsforum skal besvares med en kort forklaring. Svarene vil blive drøftet med mentoren under mentorsessionerne

1. Hvad er en VPN?
2. Hvordan kan du bruge VPN-løsningen?
3. Kan du sende din private nøgle til PGP e-mail-kryptering til nogen?

Selvevalueringsspørgsmål . Efter besvarelsen kan eleven se resultaterne og sammenligne dem med disse gemt på platformen

1. Metode til sikker adgang til dine data fra fjernadgang
2. Metoder til at sikre din e-mail-samtale

Vedhæftede filer:

1. Præsentation
2. Video film

Referencer:

1. Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam . (2021). Fælles sikkerhedsprotokoller til trådløse netværk: En sammenlignende analyse. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). En undersøgelse om trådløse sikkerhedsprotokoller (WEP, WPA og WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.
3. Kumkar , Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne , Seema. (2012). Sårbarheder i trådløse sikkerhedsprotokoller (WEP og WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.
4. Costa, Luís & Fdida , Serge & MB Duarte, Otto Carlos. (2000). En introduktion til virtuelle private netværk: mod D-VPN'er.
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