

Podstawy sieci komputerowych

Sprawozdanie z zadania 3

Łukasz Nizik
180647

Katarzyna Zychowicz
180758

ZAGADNIENIA TEORETYCZNE

1. Protokoły POP3, IMAP, SMTP, komunikacja klient-serwer, podstawowe komendy i odpowiedzi.

POP3 (Post Office Protocol v3) – protokół TCP/IP z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera na lokalny komputer (klient). Działanie protokołu powoduje pobranie wszystkich wiadomości bez znacznika *deleted* wraz z załącznikami z serwera na komputer kliencki (do maildrop) po udanej autoryzacji.

Składnia odpowiedzi serwera:

- + OK treść
- - ERR treść

Komendy:

- **QUIT** – kończy działanie, wiadomości zostają usunięte po stronie klienta.

Autoryzacja:

- **USER name**
- **PASS string**

Transakcja:

- **STAT** – sprawdzenie ilości wiadomości i rozmiaru w bajtach
- **LIST [msg]** – wyświetla informacje o wiadomości, jej numer oraz rozmiar. W przypadku bezargumentowym wyświetli informacje o wszystkich wiadomościach.
- **RETR msg** – wyświetla wiadomość.
- **DELE msg** – usuwa wiadomość.
- **NOOP** – serwer nie robi nic. Wysyła pozytywną odpowiedź bez treści.
- **RSET** – jeśli jakaś wiadomość została oznaczona przez serwer jako *deleted*, zostaje odznaczona.
- **msg** – numer wiadomości, który, jeśli istnieje, nie może odnosić się do wiadomości oznaczonej jako *deleted*.
- **[msg]** – argument nie jest obowiązkowy*

IMAP (Internet Message Access Protocol) – internetowy protokół pocztowy, zaprojektowany jako zastępca POP3. W przeciwieństwie do POP3 pozwala na zarządzanie wieloma folderami skrzynek pocztowych (mailboxes) znajdującymi się na zdalnym serwerze. Zapewnia też funkcjonalności dla klienta w trybie offline do resynchronizacji z serwerem.

IMAP4rev1 zawiera operacja dla tworzenia, usuwania i zmiany nazw skrzynek pocztowych, sprawdzania nowych wiadomości, tymczasowego usuwania wiadomości, parsowania, wyszukiwania, selektywnego pobierania atrybutów wiadomości lub tekstu.

Protokół ten używa formatów tekstowych dla komend i odpowiedzi. Dane mogą być podane w jednej z form – atom, number, string, parenthesized list, lub NIL. Dane mogą przyjmować dwie formy jednocześnie.

- **Atom** – składa się z jednego lub więcej znaków.
- **Number** – składa się z jednej lub więcej cyfr i reprezentuje wartość liczbową.
- **String** – jest ciągiem złożonym z 7 albo 8 bitowych znaków
- **Parenthesized List** – sekwencja danych rozdzielonych spacją, przechowuje struktury, może być zagnieżdżona.
- **NIL** – reprezentacja braku danych

Składnia odpowiedzi serwera:

- „OK – treść” – poprawnie wykonano polecenie
- „NO – treść” – odmowa dostępu
- „BAD – treść” – nieprawidłowe polecenie lub jego argumenty

Komendy:

- Dowolny stan:
 - **LOGOUT** – informuje serwer, że użytkownik skończył pracę z połączeniem, serwer musi wysłać wiadomość pożegnalną i przerwać połączenie.
 - **NOOP** – sprawdza informacje o nowych wiadomościach, podtrzymuje połączenie, resetując timer autologout na serwerze. Często wywoływana jest okresowo.
- Stan nieautoryzowany:
 - **STARTTLS** – rozpoczyna negocjację TLS (transport layer security), która zapobiega atakom man-in-the-middle, czyli podsłuchiowaniu i modyfikacji wiadomości przesyłanych między dwiema stronami, blokuje użycie CAPABILITY.
 - **AUTHENTICATE name** – argumentem jest nazwa mechanizmu uwierzytelniania, serwer skorzysta z niego przy logowaniu jeśli będzie on dostępny.
 - **LOGIN uname pass** – argumentami są nazwa użytkownika i hasło na serwerze. Komenda ta identyfikuje użytkownika w systemie. Hasło podawane jest jako tekst zatem korzystanie z komendy na niezabezpieczonym połączeniu grozi jego kompromitacją.
- Stan autoryzowany:
 - **SELECT mailbox** – wybiera mailbox w celu uzyskania wiadomości, znajdujących się na nim. W danym momencie może być zaznaczony tylko jeden mailbox. Symultaniczny dostęp do wielu wymaga oddzielnych połączeń. Dodatkowo serwer sprawdza i powiadamia klienta o uprawnieniach.

Przykład:

C: A142 SELECT INBOX

S: * 172 EXISTS

#liczba wiadomości w mailboxie

S: * 1 RECENT

#liczba wiadomości z flagą \Recent

S: * OK [UNSEEN 12] Message 12 is first unseen

#numer sekwencyjny pierwszej nieprzeczytanej wiadomości

S: * OK [UIDVALIDITY 3857529045] UIDs valid

#walidacja identyfikatora użytkownika

S: * OK [UIDNEXT 4392] Predicted next UID

#Przewidywane UID następnego użytkownika

S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)

#lista flag tymczasowych, które może zmienić użytkownik

S: * OK [PERMANENTFLAGS (\Deleted \Seen *)] Limited

#lista flag permanentnych, które może zmienić użytkownik (jeśli pusta, można zmienić wszystkie flagi)

S: A142 OK [READ-WRITE] SELECT completed

#informacja o zakończeniu polecenia i uprawnieniach jakie ma użytkownik w mailboxie

- **EXAMINE** – wykonuje to samo co SELECT, ale mailbox zaznaczany jest z uprawnieniami [READ-ONLY]
- **CREATE mailbox** – tworzy mailbox o zadanej nazwie, która nie figuruje jeszcze na serwerze

Przykład:

C: A003 CREATE owatagusiam/

S: A003 OK CREATE completed

- **DELETE mailbox** – usuwa istniejący mailbox o zadanej nazwie
- **RENAME mailbox newname** – zmienia nazwę istniejącego mailboxa naadaną
- **SUBSCRIBE mailbox** – dodaje nazwę mailboxa do listy „active” albo „subscribe”, którą można sprawdzić komendą LSUB
- **UNSUBSCRIBE mailbox** – odwraca skutek polecenia SUBSCRIBE
- **LIST reference mailbox** - jako argumenty przyjmuje nazwę odniesienia (np. katalog roboczy) i nazwę mailboxa. Zwraca ono listę mailboxów, które znajdują się pod daną lokacją.
- **STATUS mailbox item** – jako argumenty przyjmuje nazwę mailboxa i dane, które chcemy sprawdzić. Typy danych jakie możemy sprawdzać to MESSAGES, RECENT, UIDNEXT, UIDVALIDITY, UNSEEN, które są analogiczne do odpowiedzi na polecenie SELECT
- **APPEND mailbox literal** – dodaje sekwencję znaków jako nową wiadomość na koniec mailboxu
- **EXPUNGE** – usuwa permanentnie wszystkie wiadomości z flagą \Deleted, powiadamia o każdej usuniętej wiadomości
- **CLOSE** – to samo co EXPUNGE, ale w trybie cichym
- **SEARCH criteria** – wyszukuje wiadomości spełniające zadane kryteria

IMAP nie jest powszechnie wykorzystywany ze względu na zbyt duży stopień złożoności, oprócz wymienionych komend zawiera kilka innych, a także eksperymentalny moduł atom.

SMTP (Simple Mail Transfer Protocol) – protokół przesyłania poczty przez Internet. Proces przesyła wiadomość do innego procesu znajdującego się w obrębie tej samej sieci. Jest względnie prostym protokołem (w porównaniu do IMAP). Wysyłana jest struktura SMPT DATA, która zawiera sekcję header i body. Protokół ten oparty jest głównie o znaki ASCII.

Komendy SMTP:

- **HELO** – rozpoczyna połączenie z serwerem
- **MAIL FROM** – rozpoczyna transakcję, w której mail przesyłany jest do serwer SMTP, który może przesłać go innym mailboxów.
- **RCPT TO** – określa indywidualnego adresata
- **DATA** – dodaje wpisaną treść do bufora wiadomości, która zostanie przesłana, kolejne linijki zakończone są znakiem crlf
- **RSET** – przerywa aktualną transakcję
- **VRFY** – sprawdza czy użytkownik albo mailbox jest identyfikowany w systemie
- **QUIT** – kończy sesję

2. Protokół NNTP (Usenet)

NNTP (Network News Transfer Protocol) – protokół służący do obsługi wymiany informacji w usługach typu usenet, czyli internetowych systemów dyskusji. Sieć użytkowników może wymieniać między sobą artykuły. Między serwerami sieci usenet następuje ciągła wymiana artykułów. Klient NNTP łączy się z serwerem i może odczytywać za pośrednictwem NNTP newsy z jego dysku lokalnego.

Odpowiedzi w NNTP rozpoczynają się trzema cyframi, pierwsza oznacza postęp wykonanej komendy:

- **1xx** – wiadomość informacyjna
- **2xx** – polecenie zakończone powodzeniem
- **3xx** – wykonywanie polecenia odbywa się poprawnie, dalsze wysyłanie odpowiedzi w toku
- **4xx** – polecenie było składniowo poprawne, ale nie zostało wykonane z jakiegoś powodu
- **5xx** – nieznanne polecenie

Polecenia:

- **CAPABILITIES** – wyświetla informacje o obsługiwanych komendach
- **GROUP** – wybiera grupę
- **LAST** – gdy grupa jest wybrana, wybiera artykuł, który ma najwyższy numer w grupie (domyślnie wykonywane)
- **NEXT** – wybiera artykuł o numerze o 1 niższym
- **ARTICLE number** – wybiera artykuł o zadanym numerze
- **POST** – tworzy nowy artykuł na końcu listy
- **NEWSGROUPS** – wyświetla listę grup dostępnych na serwerze

- **QUIT** – zamyka połączenie

3. Skrzynki pocztowe, najczęściej używane parametry, adresy, aliasy

Adresy skrzynek e-mail składają się z dwóch części, lokalnej i domenowej. Są one odseparowane znakiem '@'. Domyślnie wielkość liter w adresie nie ma znaczenia.

Syntax: [local]@[domain]

Część lokalna składa się ze znaków ASCII.

Np. patrick, cesarz.neron

Część domenowa jest adresem IP serwera wymiany poczty. Może być reprezentowana przez nazwę hosta, lub alias.

Np. [192.168.0.251], example.com

W adresie dozwolone są komentarze, które podaje się w nawiasach na początku, lub na końcu nazwy lokalnej oraz domenowej np. (komentarz) patric@example.com

Najczęściej parametrami kont pocztowych są login (adres) i hasło, port (od niego zależy wykorzystywany protokół).

- POP3 - port 110
- IMAP - port 143
- SMTP - port 25

Alias e-mail – alternatywne adresy e-mail wskazujące na istniejący adres podstawowy. Można nazwać je pseudonimami. Aliasy dzielimy na ogólne i pojedyncze. Ogólne dotyczą wszystkich wiadomości przychodzących na adres, który nie jest aliasem pojedynczym. Pojedyncze dotyczą jednej konkretnej skrzynki pocztowej.

4. Format przesyłki pocztowej, separator nagłówka i treści, nazwy i znaczenie podstawowych znaczników (pól) nagłówka

Przesyłka pocztowa składa się z pól nagłówka (header fields) i treści (body). Linijka przesyłki nie może mieć więcej niż 998 znaków bez znacznika końca linii (CRLF).

Pola nagłówka składają się z nazwy pola znaku ':' i treści pola.

Podstawowe pola nagłówka:

- **orig-date** – data nadania
- **from** – adres i dane autora wiadomości

- **to** – adres odbiorcy
- **subject** – temat wiadomości
- **reply-to** – adres, na który można odpowiedzieć na wiadomość
- **sender** – adres, z którego wiadomość została wysłana
- **message-ID** – unikatowy numer identyfikujący wiadomość w skrzynce
- **in-reply-to** – wiadomość jest odpowiedzią na wiadomość o zadanym ID
- **content-type** – standard formatowania użyty dla wiadomości (np. MIME)

Treść przesyłki jest po prostu linijkami zawierającymi znaki ASCII, zwykle dozwolone jest wysyłanie danych binarnych, oraz formatowania html.

5. Załączniki, kodowanie, MIME

MIME (ang. Multipurpose Internet Mail Extensions) to standard stosowany przy przesyłaniu poczty elektronicznej (ang. e-mail). MIME definiuje budowę komunikatu poczty elektronicznej.

Wiadomość w formacie MIME składa się z nagłówków i treści. Nagłówki określają różne parametry związane z przesyłaną wiadomością, takie jak nadawcę, temat, odbiorcę, rodzaj zawartości, kodowanie transportowe (określające sposób zamiany danych 8-bitowych – jak np. pliki binarne, zdjęcia, filmy, dźwięk – do formatu 7-bitowych danych w standardzie ASCII).

Podstawowy protokół przesyłania wiadomości e-mail, SMTP, wspiera tylko 7-bitowe znaki ASCII. Powoduje to ograniczenie poczty elektronicznej do wiadomości, które zawierają tylko znaki wystarczające do pisania w niewielkiej ilości języków, głównie w angielskim. Inne języki bazujące na alfabecie łacińskim zazwyczaj zawierają znaki diakrytyczne, które nie są wspierane przez 7-bitowe ASCII, co sprawia, że tekst w tych językach nie może być poprawnie reprezentowany w podstawowej wiadomości e-mail.

MIME definiuje mechanizmy do przesyłania innego rodzaju informacji wewnątrz wiadomości e-mail:

- tekstu w językach używających innego kodowania znaków niż ASCII,
- 8-bitowych danych binarnych, takich jak pliki zawierające obrazy, dźwięki i filmy, a także programy komputerowe.

Podstawowy standard poczty elektronicznej określa następujące nagłówki wiadomości e-mail: "To:", "Subject:", "From:" oraz "Date:". Określają one adresata wiadomości, jej temat, nadawcę oraz datę wysłania. MIME określa zaś zbiór nagłówków e-mail służących do określenia dodatkowych atrybutów wiadomości, włączając w to rodzaj zawartości (zwany "typem MIME"), oraz definiuje zbiór metod kodowania transportowego, które mogą być użyte do reprezentowania 8-bitowych danych binarnych przy użyciu znaków z 7-bitowego zbioru znaków ASCII. MIME określa również zasady kodowania znaków spoza ASCII wewnątrz nagłówków wiadomości e-mail, takich jak "Subject:", pozwalając tym nagłówkom na zawieranie takich znaków.

Nagłówki MIME

- **MIME-Version** - obecność tego nagłówka wskazuje, że wiadomość jest sformatowana zgodnie z MIME. Typowa wartość to "1.0".

- **Content-ID** - nagłówek jest używany głównie w wiadomościach wieloczęściowych. Jest to unikatowy identyfikator części wiadomości, pozwalający na odwoływanie się do niej.
- **Content-Type** - ten nagłówek wskazuje typ MIME zawartości wiadomości. Składa się z typu i podtypu.
 - Nazwa typu mediów:
 - text
 - image
 - audio
 - video
 - application

Dopuszcza się czasem jeszcze dwie wartości: multipart i message. Przez użycie typu multipart, MIME pozwala, by wiadomość posiadała wiele części, z których każda może mieć określony swój własny typ MIME.

- Nazwa podtypu, np. xhtml+xml lub plain itp.
- Wymagane parametry (nie każdy typ tego wymaga)
- Opcjonalne parametry (nie każdy typ tego wymaga), np. charset="us-ascii"
- **Content-Disposition** - określa sposób prezentacji wiadomości. Każda część wiadomości w formacie MIME może mieć:
 - styl inline, czyli treść powinna być automatycznie wyświetlana wewnątrz wiadomości; lub
 - styl attachment, w przypadku którego treść nie jest wyświetlana automatycznie, lecz wymaga jakiejś akcji ze strony użytkownika, by ją otworzyć (czyli popularne załączniki).

Oprócz stylu prezentacji, nagłówek Content-Disposition dostarcza także pól do określenia nazwy pliku, daty jego utworzenia i daty modyfikacji, które mogą być użyte przez klienta do zapisania załącznika.

- **Content-Transfer-Encoding** - Określa sposób reprezentacji danych binarnych przy użyciu siedmiobitowych znaków ASCII. Nagłówek Content-Transfer-Encoding spełnia dwie funkcje:
 - Wskazuje czy zastosowano kodowanie danych binarnych do postaci tekstowej oprócz oryginalnego kodowania określonego w nagłówku Content-Type (np. UTF-8); oraz
 - Jeżeli taka metoda kodowania danych binarnych do postaci tekstowej została użyta, wskazuje która to metoda.

6. Pocztowe listy dystrybucyjne, bramy pocztowe

Lista dystrybucyjna to lista internetowych adresów e-mail, która służy do masowego rozsyłania listów do osób, których adresy znajdują się na liście. Listy dystrybucyjne są stosowane w wielu różnych celach. Służą one m.in. do rozsyłania czasopism internetowych, newsletterów, reklamy, oraz niestety także spamu.

Podział:

- **listy pop-in** - są to listy, do których trzeba się świadomie zapisać z własnej inicjatywy, lub przynajmniej wyrazić zgodę na zapisanie.

- **listy pop-out** - są to zwykle listy gromadzone automatycznie (choć czasem też ręcznie), z których jednak istnieje rzeczywiście możliwość wypisania się. Adresy są dopisywane do listy bez zgody czy nawet świadomości właściciela danego adresu i dowiaduje się on o tym fakcie zwykle w momencie otrzymania pierwszego maila wysłanego z takiej listy.
- **listy profilowane** - na takie listy trafia się zwykle po wypełnieniu specjalnie do tego celu przygotowanej ankiety. Listy takie zawierają adresy osób wyselekcjonowanych wg jakiegoś kryterium.
- **listy wstępnie weryfikowane** - listy takie zawierają dość przypadkowe adresy e-mail, o których wiadomo tylko tyle, że są aktywne. Są one często niemal tożsame z listami automatycznymi weryfikowanymi i jedyna różnica polega na tym, że można się z takiej listy wypisać.
- **listy automatyczne, nie weryfikowane** - są one tworzone przez specjalne programy, które skanują strony WWW, fora dyskusyjne, Usenet a nawet e-mailowe listy dyskusyjne w poszukiwaniu adresów e-mail.
- **listy automatyczne, zweryfikowane** - są to listy gromadzone w sposób podobny do list całkowicie automatycznych, ale zanim dany adres trafi na taką listę, jest weryfikowany poprzez automat, który wysłał mail na dany adres z prośbą o odpowiedź. W liście służącym do weryfikacji jest zazwyczaj pytanie o to, czy dana osoba życzy sobie być dopisana do listy.

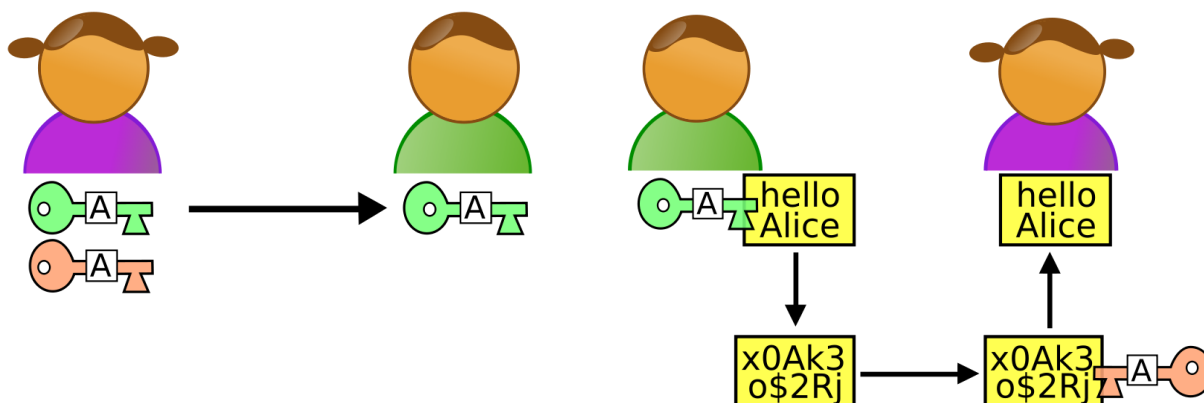
Brama pocztowa (ang. mail gateway) - serwer łączący dwa lub więcej systemów poczty elektronicznej i przesyłający komunikaty między nimi.

7. Bezpieczeństwo usług pocztowych, szyfrowanie połączeń, bezpieczne uwierzytelnianie, szyfrowanie zawartości, użycie kluczy niesymetrycznych, PGP, certyfikaty SSL, podpis elektroniczny.

Szyfrowanie

Jednym z podstawowych problemów dla stosowania szyfrowania w sieci Internet jest wymiana kluczy szyfrowych. W tradycyjnych metodach szyfrowania - tzw. **szyfrach symetrycznych** - nadawca i odbiorca zaszyfrowanej informacji muszą dysponować tym samym kluczem, aby rezultat odszyfrowania pokrył się z informacją, która została zaszyfrowana. Tym samym, klucz szyfrowania musi być uprzednio ustalony, np. przesłany jednej stronie przez drugą z użyciem tzw. kanału bezpiecznego (tzn. w sposób zapewniający poufność). W Internecie rozwiązanie takie jest mało praktyczne, gdyż dla stron komunikujących się przez sieć często jest ona jedynym dostępnym kanałem wymiany informacji i tym samym bezpieczna (poufna) wymiana klucza jest niemożliwa. Metodą na rozwiązanie tego problemu było stworzenie nowej dziedziny kryptografii, mianowicie **szyfrów niesymetrycznych** i metody **kluczy publicznych**.

Kryptografia asymetryczna to rodzaj kryptografii, w którym używa się zestawów dwu lub więcej powiązanych ze sobą kluczy, umożliwiających wykonywanie różnych czynności kryptograficznych. Jeden z kluczy może być udostępniony publicznie bez utraty bezpieczeństwa danych zabezpieczanych tym kryptosystemem.



Przekazanie klucza publicznego (kolor zielony) drugiemu użytkownikowi. Klucz prywatny (kolor czerwony) pozostaje tajny.

Użytkownik używa klucza publicznego, aby zaszyfrować wiadomość. Klucz prywatny wykorzystywany jest do odszyfrowania.

Najważniejsze zastosowania kryptografii asymetrycznej – szyfrowanie i podpisy cyfrowe – zakładają istnienie 2 kluczy – prywatnego i publicznego, przy czym klucza prywatnego nie da się łatwo odtworzyć na podstawie publicznego. Algorytmy mające zastosowanie w kryptografii asymetrycznej wykorzystują operacje jednokierunkowe - takie, które da się łatwo przeprowadzić w jedną stronę, a bardzo trudno w drugą.

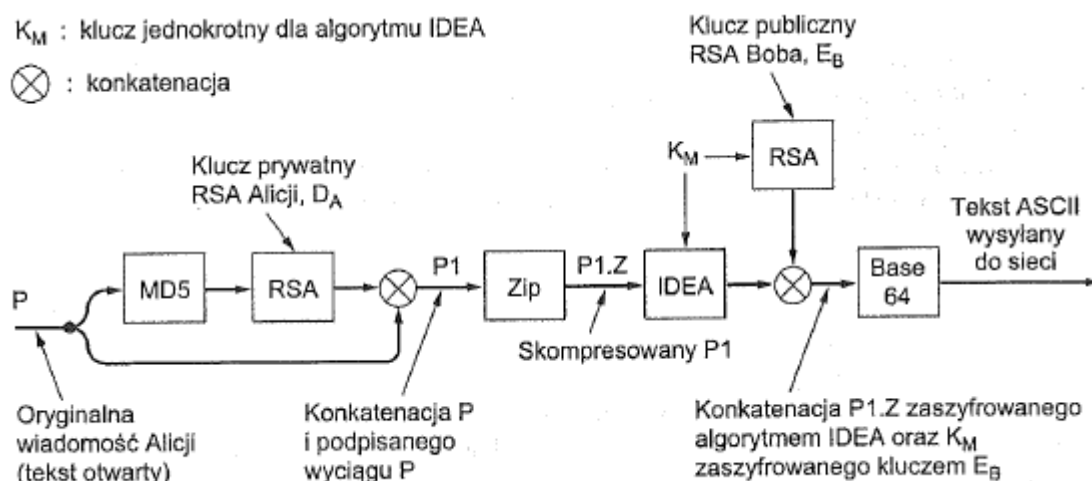
Klucz publiczny używany jest do zaszyfrowania informacji, klucz prywatny do jej odczytu. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji, tylko on może ją odczytać. Natomiast klucz publiczny jest udostępniony każdemu, kto zechce zaszyfrować wiadomość.

Ponieważ kryptografia asymetryczna jest o wiele wolniejsza od symetrycznej, prawie nigdy nie szyfruje się wiadomości za pomocą kryptosystemów asymetrycznych. Zamiast tego szyfruje się jedynie klucz jakiegoś szyfru symetrycznego, takiego jak np. AES. Takie protokoły, łączące elementy kryptografii symetrycznej i asymetrycznej, nazywa się hybrydowymi.

Pretty Good Privacy (w skrócie PGP) – to jedno z najpopularniejszych narzędzi do szyfrowania poczty elektronicznej. PGP pozwala szyfrować i deszyfrować przesyłane wiadomości, podpisywać je cyfrowo, weryfikować autentyczność nadawcy (pod warunkiem że ten także korzysta z PGP) i zarządzać kluczami.

Na potrzeby szyfrowania PGP wykorzystuje algorytm IDEA (International Data Encryption System) używający 128-bitowych kluczy. Na potrzeby zarządzania kluczami wykorzystuje się algorytm RSA (jeden z pierwszych i obecnie najpopularniejszych algorytmów kryptografii asymetrycznej), natomiast w celu zachowania integralności danych PGP posługuje się funkcją MD5.

PGP nie zawiera żadnych elementów poczty elektronicznej – dostarcza tylko zaszyfrowane, podpisane teksty. Oczywiście tekst taki można swobodnie przesyłać e-mailem, do czego PGP jest powszechnie wykorzystywane.



SSL - protokół służący do szyfrowania transmisji danych w sieci Internet. SSL może być stosowany zarówno do zabezpieczenia przesyłania danych ze strony WWW (np. formularz z danymi osobowymi, panel administracyjny, obsługa konta bankowego), jak i poczty elektronicznej (wysyłka i odbiór poczty). W momencie uruchomienia szyfrowania wszelkie dane przesyłane na linii użytkownik - serwer są kodowane. Moc szyfrowania (zazwyczaj 128 bitów) praktycznie uniemożliwia podsłuchanie transmisji. Certyfikat (bezpieczne uwierzytelnianie) to swoisty dokument tożsamości serwera WWW. Oprócz funkcji zabezpieczającej, pełni on obecnie rolę autoryzującą.

Certyfikat SSL może zostać zainstalowany dla serwera, który dysponuje adresem IP. Dla jednego adresu IP może zostać uruchomiony tylko jeden certyfikat. Certyfikat wystawiany jest dla jednej, konkretnej domeny. Pamiętać należy, że w tym wypadku ma znaczenie, czy używana jest domena np. z przedrostkiem www, czy też bez niego.

- **RapidSSL** - najprostszy, wystawiany przez Equifax Secure eBusiness, 128-bitowy, rozpoznawalny przez 96% obecnie używanych przeglądarek
- **QuickSSL** - certyfikat profesjonalny, gwarantujący wysokie zaufanie, wystawiany przez GeoTrust, 128-bitowy, rozpoznawalny przez 98% obecnie używanych przeglądarek WWW

Podpis cyfrowy (podpis elektroniczny) to dodatkowa informacja dołączona do wiadomości służąca do weryfikacji jej źródła. Podpis elektroniczny służy zapewnieniu następujących funkcji:

- autentyczności, czyli pewności co do autorstwa dokumentu,
- niezaprzeczalności, czyli pewności, że to osoba podpisana stworzyła dokument,
- integralności, czyli pewności, że wiadomość nie została zmodyfikowana po złożeniu podpisu przez autora.

8. Netykieta, tzw. spam, tzw. czarne listy

Netykieta – zbiór zasad przyzwoitego zachowania w Internecie, swoista etykieta obowiązująca w sieci. Netykieta, podobnie jak zwykłe zasady przyzwoitego zachowania, nie jest dokładnie skodyfikowana. Zasady netykiety wynikają wprost z ogólnych zasad przyzwoitości lub są odzwierciedleniem niemożliwych do ujęcia w standardy ograniczeń technicznych wynikających z natury danej usługi Internetu.

Spam to elektroniczne wiadomości rozsyłane do osób, które ich nie oczekują. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty elektronicznej oraz w Usenecie. Zwykle (choć nie zawsze) jest wysyłany masowo. Istotą spamu jest rozsyłanie dużej liczby informacji komercyjnych o jednakowej treści do nieznanym sobie osób. Nie ma znaczenia jaka jest treść tych wiadomości. By wiadomość określić mianem spamu musi ona spełnić trzy następujące warunki jednocześnie:

1. treść wiadomości jest niezależna od tożsamości odbiorcy;
2. odbiorca nie wyraził uprzedniej, zamierzonej zgody na otrzymanie tej wiadomości;
3. treść wiadomości daje podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy.

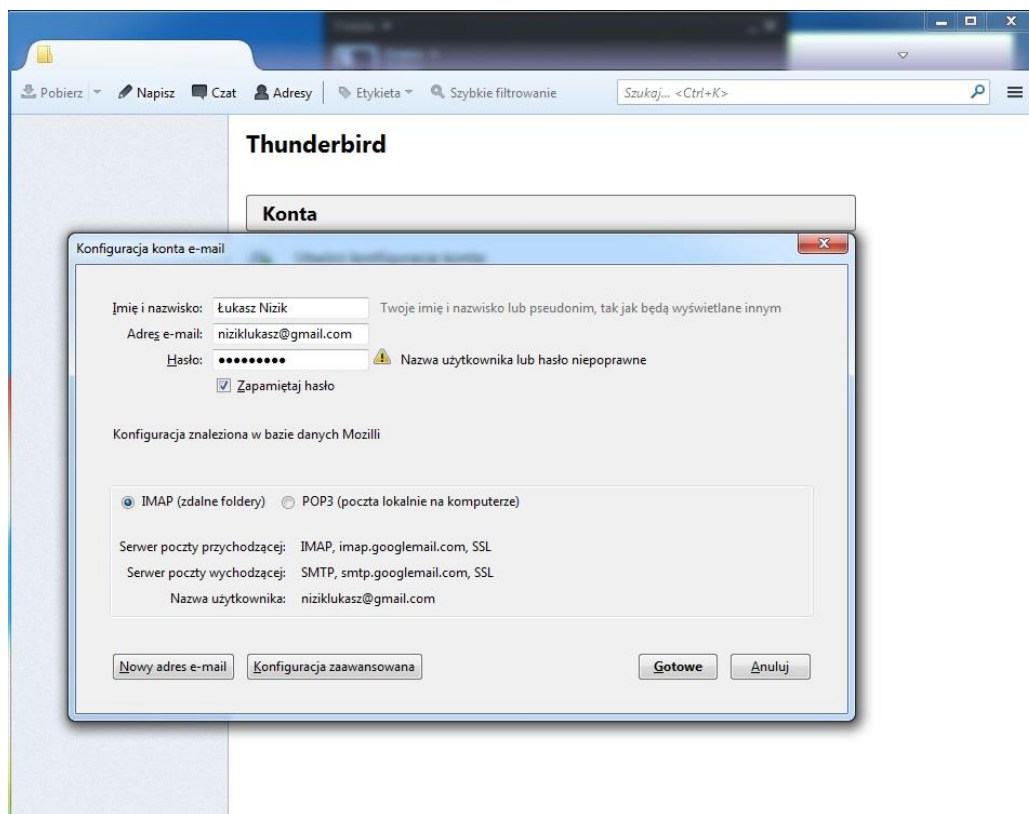
Czarna lista (ang. black list) – Czarne listy są zazwyczaj bardzo duże i wbudowane bezpośrednio w poszczególne aplikacje. W wypadku programów antyspamowych, na czarnej liście znajdują się adresy IP i e-mail, które wysyłają duże ilości spamu. Dla efektywnego działania konieczne jest regularne aktualizowanie czarnych list tak, aby oprogramowanie mogło skutecznie chronić komputer przed niechcianymi treściami, na przykład spamem.

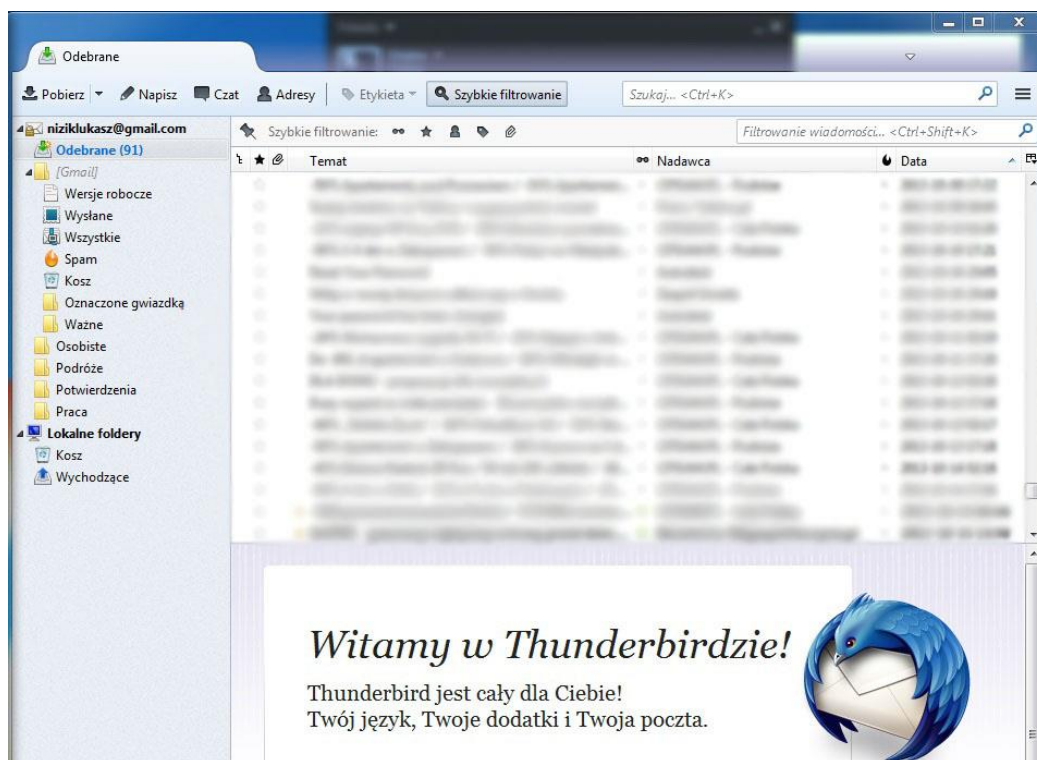
Bibliografia:

- A. S. Tannenbaum “Sieci komputerowe”, 2004 Helion
- POP3 <http://www.rfc-editor.org/rfc/rfc1939.txt>
- IMAP <http://www.rfc-editor.org/rfc/rfc3501.txt>
- SMTP <http://www.rfc-editor.org/rfc/rfc2821.txt>
- http://en.wikipedia.org/wiki/Network_News_Transfer_Protocol
- NNTP <http://www.rfc-editor.org/rfc/rfc3977.txt>
- http://en.wikipedia.org/wiki/Email_address
- <https://support.google.com/a/answer/33327?hl=pl>
- Format e-mail, pola nagłówka <http://www.rfc-editor.org/rfc/rfc5322.txt>
- MIME http://pl.wikipedia.org/wiki/Multipurpose_Internet_Mail_Extensions
- <http://www.e-mailmarketing.biz/wiki.htm>
- <http://home.agh.edu.pl/~szymon/artykuly/kryptografia.html>
- PGP http://helionica.pl/index.php/Pretty_Good_Privacy
- SSL <https://pero.wpw.pl/>
- <http://pl.wikipedia.org/wiki/Netykieta>
- <http://poczta.onet.pl/pomoc/13976,slownik.html>
- http://pl.wikipedia.org/wiki/Czarna_lista

ZADANIA PRAKTYCZNE

1. Skonfigurować program Thunderbird do pracy z własnym kontem pocztowym na serwerze stud.ics.p.lodz.pl lub na dowolnym innym serwerze.





Nie napotkałem trudności w przeprowadzeniu wymaganego procesu, program automatycznie wykrył dostępne konfiguracje i pozwolił na wybranie jednej z nich (IMAP albo POP3). Po zaakceptowaniu, wiadomości i struktura skrzynki zostały automatycznie pobrane z serwera i wyświetlone w aplikacji.

2. Wysłać wiadomości pocztowe

a. na nieistniejący serwer pocztowy (nieprawidłowa nazwa DNS)

Adres odbiorcy: manamana@nieistniejacyserverpocztowyatall.naprawde

Odpowiedź serwera:

Delivery to the following recipient failed permanently:

manamana@nieistniejacyserverpocztowyatall.naprawde

Technical details of permanent failure:

DNS Error: Domain name not found

----- Original message -----

[...]

X-Received: by 10.180.74.174 with SMTP id u14mr3809626wiv.45.1385293299241;
Sun, 24 Nov 2013 03:41:39 -0800 (PST)s

Return-Path: niziklukasz@gmail.com

Received: from [192.168.1.89] (178-37-244-168.adsl.inetia.pl.
[178.37.244.168])

by mx.google.com with ESMTPSA id
f11sm18174976wic.4.2013.11.24.03.41.37

for manamana@nieistniejacyserverpocztowyatall.naprawde
(version=TLSv1 cipher=ECDHE-RSA-RC4-SHA bits=128/128);

Sun, 24 Nov 2013 03:41:38 -0800 (PST)

Message-ID: 5291E5F2.10407@gmail.com

Date: Sun, 24 Nov 2013 12:41:38 +0100

From: =?UTF-8?B?xYF1a2FzeiBOaXppaw==?= <niziklukasz@gmail.com>
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101
Thunderbird/24.1.1
MIME-Version: 1.0
To: manamana@nieistniejacyserwerpocztowyatall.naprawde
Subject: Temat testowy
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit

Wiadomość email.

b. do nieistniejącego użytkownika na istniejącym serwerze pocztowym

Odpowiedź serwera:

Delivery to the following recipient failed permanently:

[wiedzetenadresemailnieistniejaaleitakwyslenaniegowiadomosczebypokazacmojaodrebnosc@gmail.com](mailto:wiemzetenadresemailnieistniejaaleitakwyslenaniegowiadomosczebypokazacmojaodrebnosc@gmail.com)

Technical details of permanent failure:
Google tried to deliver your message, but it was rejected by the server for the recipient domain gmail.com by gmail-smtp-in.l.google.com.
[2a00:1450:400c:c05::1b].

The error that the other server returned was:

550-5.1.1 The email account that you tried to reach does not exist. Please try

550-5.1.1 double-checking the recipient's email address for typos or

550-5.1.1 unnecessary spaces. Learn more at

550 5.1.1 <http://support.google.com/mail/bin/answer.py?answer=6596>

hh8sil6111976wjc.166 - gsmtip

----- Original message -----

[...]

X-Received: by 10.180.198.79 with SMTP id

ja15mr9556156wic.36.1385293626574;

Sun, 24 Nov 2013 03:47:06 -0800 (PST)

Return-Path: <niziklukasz@gmail.com>

Received: from [192.168.1.89] (178-37-244-168.adsl.inetia.pl.

[178.37.244.168])

by mx.google.com with ESMTPSA id

hv5sm35145587wib.2.2013.11.24.03.47.05

for

<wiedzetenadresemailnieistniejaaleitakwyslenaniegowiadomosczebypokazacmojaodrebnosc@gmail.com>

(version=TLSv1 cipher=ECDHE-RSA-RC4-SHA bits=128/128);

Sun, 24 Nov 2013 03:47:05 -0800 (PST)

Message-ID: <5291E73A.6090604@gmail.com>

Date: Sun, 24 Nov 2013 12:47:06 +0100

From: =?UTF-8?B?xYF1a2FzeiBOaXppaw==?= <niziklukasz@gmail.com>

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101

Thunderbird/24.1.1

MIME-Version: 1.0

To:

wiedzetenadresemailnieistniejaaleitakwyslenaniegowiadomosczebypokazacmojaodrebnosc@gmail.com

Content-Type: text/plain; charset=UTF-8; format=flowed

Content-Transfer-Encoding: 8bit

Ta wiadomość i tak do nikogo nie trafi. Nie wiem po co wgl. to robię.

c. do komputera, który istnieje, ale nie działa na nim serwer poczty

Odpowiedź serwera:

Delivery to the following recipient failed permanently:

gigabajka@platige.com

Technical details of permanent failure:

Google tried to deliver your message, but it was rejected by the server for the recipient domain platige.com by lila.platige.com. [193.192.62.146].

The error that the other server returned was:

550 5.1.1 [<gigabajka@platige.com>](mailto:gigabajka@platige.com): Recipient address rejected: User unknown in local recipient table

----- Original message -----

[...]

X-Received: by 10.180.37.11 with SMTP id u11mr9603209wij.27.1385294393262;
Sun, 24 Nov 2013 03:59:53 -0800 (PST)

Return-Path: [<niziklukasz@gmail.com>](mailto:niziklukasz@gmail.com)

Received: from [192.168.1.89] (178-37-244-168.adsl.inetia.pl.
[178.37.244.168])

by mx.google.com with ESMTPSA id
s2sm35549402wiw.7.2013.11.24.03.59.52

for [<gigabajka@platige.com>](mailto:gigabajka@platige.com)

(version=TLSv1 cipher=ECDHE-RSA-RC4-SHA bits=128/128);

Sun, 24 Nov 2013 03:59:52 -0800 (PST)

Message-ID: [<5291EA39.5000006@gmail.com>](mailto:5291EA39.5000006@gmail.com)

Date: Sun, 24 Nov 2013 12:59:53 +0100

From: =?UTF-8?B?xYFla2FzeiBOaXppaw==?= [<niziklukasz@gmail.com>](mailto:niziklukasz@gmail.com)

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101

Thunderbird/24.1.1

MIME-Version: 1.0

To: gigabajka@platige.com

Subject: Checking if MX server exists

Content-Type: text/plain; charset=UTF-8; format=flowed

Content-Transfer-Encoding: 7bit

None

Czas po jakim otrzymałem odpowiedzi od serwera poczty google to 0.9 s (+- 0.1 s). Nie jest podana ilość prób wysłania wiadomości przez serwer. W odpowiedzi udzielone zostały informacje o serwerze poczty („moim”) czyli mx.google.com, o fakcie korzystania z klienta poczty Thunderbird, sposobie kodowania wiadomości (UTF-8), ID wiadomości, czasie nadania. W punktach b i c otrzymałem też adres ip domeny serwera odbiorcy.

3. Za pomocą programu *windump* i/lub *ethereal* przeanalizować zawartość nagłówków pakietów TCP przesyłanych między klientem a serwerem poczty.

3	0.004087000	172.20.56.229	193.17.41.99	TCP	66 49396 > submission [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.014030000	193.17.41.99	172.20.56.229	TCP	66 submission > 49396 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
5	0.014106000	172.20.56.229	193.17.41.99	TCP	54 49396 > submission [ACK] Seq=1 Ack=1 win=65700 Len=0
6	0.022710000	193.17.41.99	172.20.56.229	SMTP	83 S: 220 poczta.o2.pl ESMTP wita
7	0.057655000	172.20.56.229	193.17.41.99	SMTP	72 C: EHLO [127.0.0.1]
8	0.064789000	193.17.41.99	172.20.56.229	TCP	54 submission > 49396 [ACK] Seq=30 Ack=19 win=5888 Len=0
9	0.064962000	193.17.41.99	172.20.56.229	SMTP	164 S: 250 poczta.o2.pl 250 SIZE 150000000 250 AUTH LOGIN PLAIN 250 AUTH LOGIN PLAIN 250 STARTTLS 250 8BITMIME
10	0.066733000	172.20.56.229	193.17.41.99	SMTP	99 C: AUTH PLAIN AG1hcnRpbjc4NwBTRlNQSnVuaw9yMjY=
11	0.080655000	193.17.41.99	172.20.56.229	SMTP	84 S: 235 Authentication succeeded
12	0.085787000	172.20.56.229	193.17.41.99	SMTP	92 C: MAIL FROM:<katarzyna.zychowicz@o2.pl> SIZE=394
13	0.100596000	193.17.41.99	172.20.56.229	SMTP	62 S: 250 ok
14	0.102172000	172.20.56.229	193.17.41.99	SMTP	90 C: RCPT TO:<elejedor@gmail.com>
15	0.110089000	193.17.41.99	172.20.56.229	SMTP	62 S: 250 ok
16	0.114949000	172.20.56.229	193.17.41.99	SMTP	60 C: DATA
17	0.122775000	193.17.41.99	172.20.56.229	SMTP	82 S: 354 end with <CRLF>.<CRLF>
18	0.133222000	172.20.56.229	193.17.41.99	IMF	544 from: =?UTF-8?B?TWYyZ2luIFNOYcWEY3phaw==?= <katarzyna.zychowicz@o2.pl>, subject: Email, (text/plain)
19	0.179769000	193.17.41.99	172.20.56.229	TCP	54 submission > 49396 [ACK] Seq=214 Ack=634 win=6912 Len=0
20	1.623669000	193.17.41.99	172.20.56.229	SMTP	79 S: 250 OK queued as xdfjan
21	1.626071000	172.20.56.229	193.17.41.99	SMTP	60 C: QUIT
22	1.633112000	193.17.41.99	172.20.56.229	TCP	54 submission > 49396 [ACK] Seq=239 Ack=640 win=6912 Len=0
23	1.633305000	193.17.41.99	172.20.56.229	SMTP	62 S: 250 ok
24	1.633708000	193.17.41.99	172.20.56.229	SMTP	109 S: 221 poczta.o2.pl Service closing transmission channel
25	1.633791000	172.20.56.229	193.17.41.99	TCP	54 49396 > submission [ACK] Seq=640 Ack=303 win=65396 Len=0
26	1.634532000	172.20.56.229	193.17.41.99	TCP	54 49396 > submission [FIN, ACK] Seq=640 Ack=303 win=65396 Len=0
27	1.644413000	193.17.41.99	172.20.56.229	TCP	54 submission > 49396 [ACK] Seq=303 Ack=641 win=6912 Len=0

Następuje wymiana pakietów SYN oraz SYN-ACK w celu synchronizacji.

4. Wysłać i odebrać wiadomość łącząc się z serwerem poczty za pomocą dowolnego klienta protokołu telnet.

Uwierzytelnianie

```
Telnet stud.ics.p.lodz.pl

Politechnika Lodzka
Instytut Informatyki

Technical University of Lodz, Poland
Institute of Computer Science

Linux 2.6.## on an i686

Witamy na
stud.ics.p.lodz.pl

Welcome to stud.ics.p.lodz.pl

login: elejedor
Password:

Instytut Informatyki Politechniki Lodzkiej w Lodzi
Wolczanska 215
90-924 Lodz

*
* Zasady korzystania z powloki, poczty, www, mysql itp.
* patrz: http://ics.p.lodz.pl/zasady/inet
*

[elejedor@stud ~]$
```

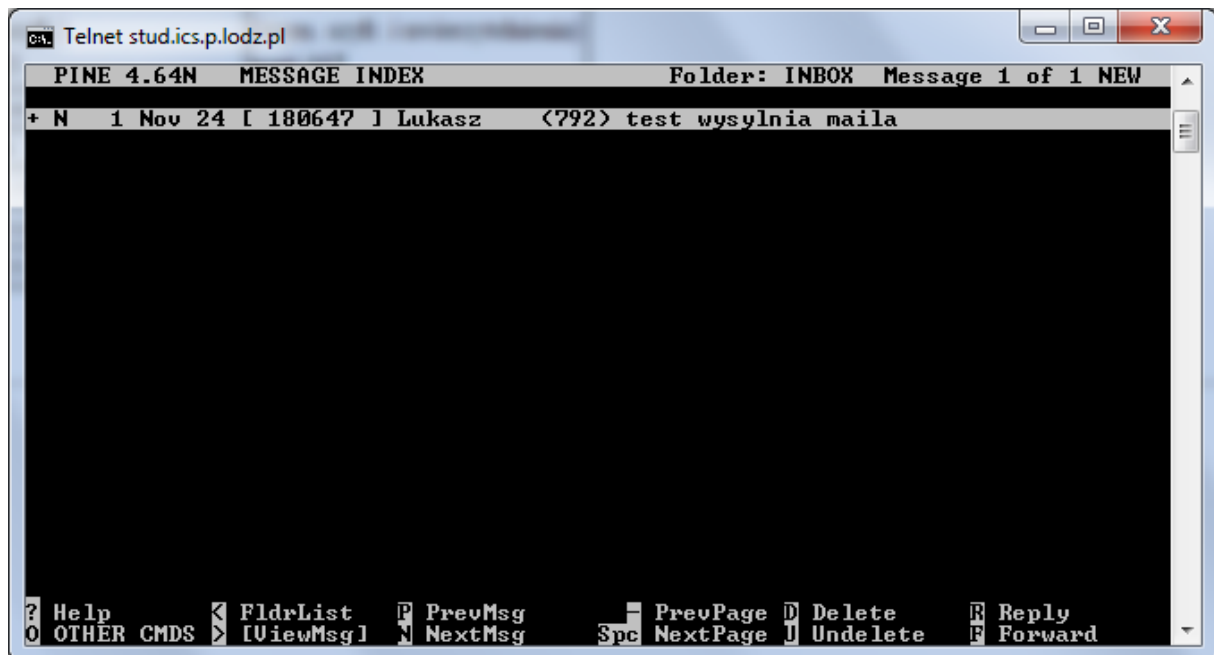
Wysyłanie wiadomości za pomocą polecenia pine [adres email]

```
Telnet stud.ics.p.lodz.pl

PINE 4.64N      COMPOSE MESSAGE      Folder: <CLOSED>  No Messages

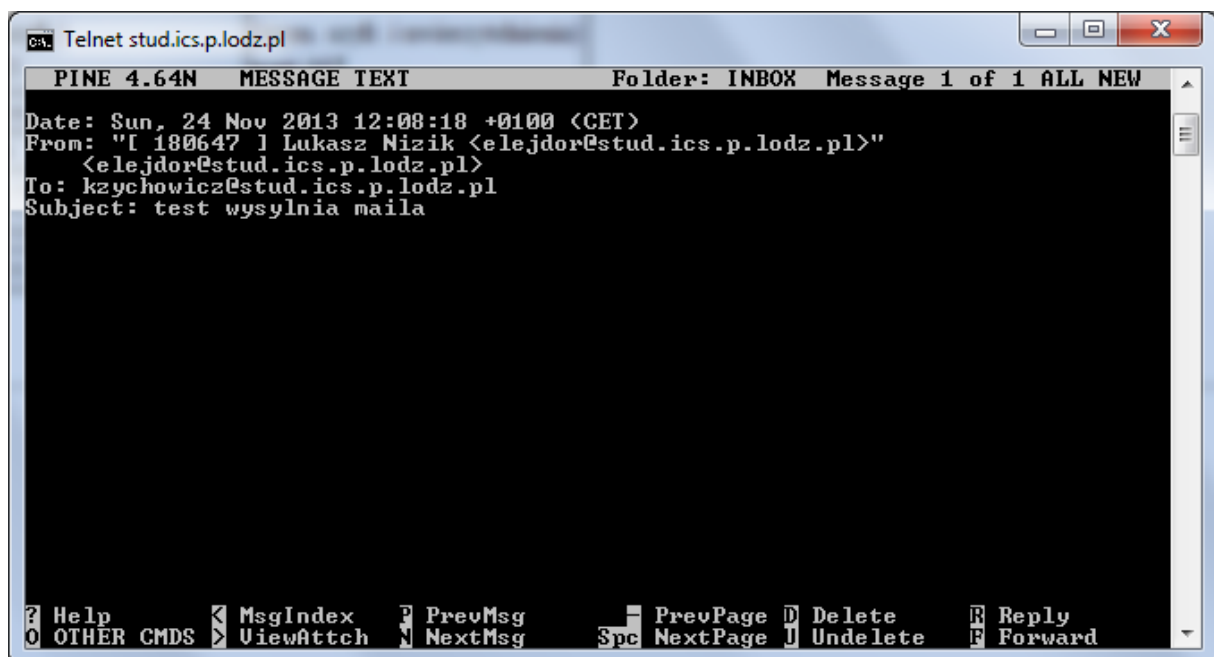
From : "[I 180647 I Lukasz Nizik <elejedor@stud.ics.p.lodz.pl>" <elejedor@stud.ics.p.lodz.pl>
To : kzychowicz@stud.ics.p.lodz.pl
Cc :
Attchmnt:
Subject : test wysylnia maila
----- Message Text -----
```


Pobieranie wiadomości za pomocą polecenia pine bez parametrów



```
Telnet stud.ics.p.lodz.pl
PINE 4.64N  MESSAGE INDEX  Folder: INBOX  Message 1 of 1 NEW
+ N  1 Nov 24 [ 180647 ] Lukasz  <792> test wysylnia maila

? Help      FldrList  PrevMsg    PrevPage  Delete    Reply
0 OTHER CMDS [ViewMsg] NextMsg    Spc       NextPage  Undelete  Forward
```



```
Telnet stud.ics.p.lodz.pl
PINE 4.64N  MESSAGE TEXT  Folder: INBOX  Message 1 of 1 ALL NEW
Date: Sun, 24 Nov 2013 12:08:18 +0100 (CET)
From: "[ 180647 ] Lukasz Nizik <elejdor@stud.ics.p.lodz.pl>"
      <elejdor@stud.ics.p.lodz.pl>
To: kzychowicz@stud.ics.p.lodz.pl
Subject: test wysylnia maila

? Help      MsgIndex  PrevMsg    PrevPage  Delete    Reply
0 OTHER CMDS ViewAttch NextMsg    Spc       NextPage  Undelete  Forward
```

Telnet jest standardem protokołu komunikacyjnego. Programy w wersji konsolowej do jego obsługi dostarczone są z systemem windows 7. W zadaniu użyty był klient telnet do przesłania i odebrania wiadomości z pośrednictwem uczelnianego serwera.

5. Przesłać wiadomość zaszyfrowaną/podpisaną za pomocą PGP/certyfikatu SSL i przeanalizować podsłuch tej transmisji za pomocą programu ethereal.

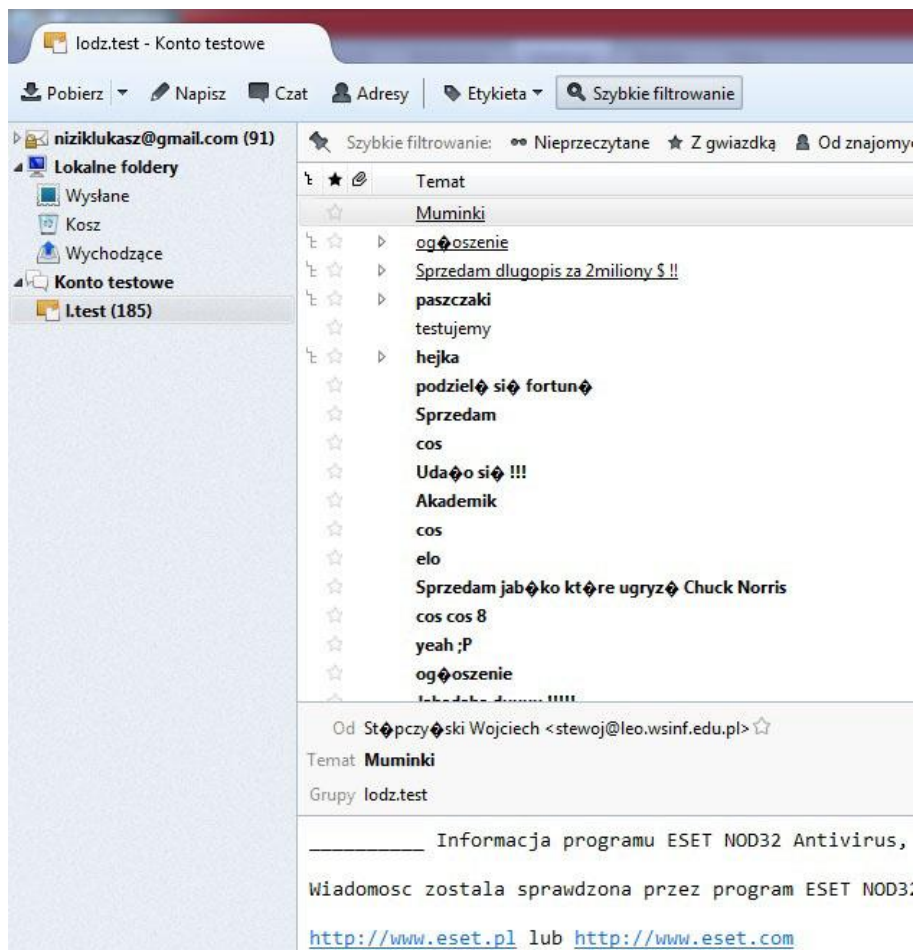
No.	Time	Source	Destination	Protocol	Length	Info
121	6.035092000	192.168.1.89	173.194.66.16	TCP	66	iax > urd [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
122	6.091186000	173.194.66.16	192.168.1.89	TCP	66	urd > iax [SYN, ACK] Seq=0 Ack=1 win=62920 Len=0 MSS=1430 SACK_PERM=1 WS=64
123	6.091263000	192.168.1.89	173.194.66.16	TCP	54	iax > urd [ACK] Seq=1 Ack=1 win=65780 Len=0
124	6.091508000	192.168.1.89	173.194.66.16	TLSv1	438	Client Hello
125	6.149545000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [ACK] Seq=1 Ack=385 win=64000 Len=0
126	6.167798000	173.194.66.16	192.168.1.89	TLSv1	187	Server Hello, Change Cipher Spec, Encrypted Handshake Message
127	6.168157000	192.168.1.89	173.194.66.16	TLSv1	101	Change Cipher Spec, Encrypted Handshake Message
131	6.235834000	173.194.66.16	192.168.1.89	TLSv1	131	Application Data
132	6.240580000	192.168.1.89	173.194.66.16	TLSv1	100	Application Data
133	6.306325000	173.194.66.16	192.168.1.89	TLSv1	259	Application Data
134	6.317814000	192.168.1.89	173.194.66.16	TLSv1	136	Application Data
136	6.412200000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [ACK] Seq=416 Ack=560 win=64000 Len=0
144	6.787148000	173.194.66.16	192.168.1.89	TLSv1	99	Application Data
145	6.787884000	192.168.1.89	173.194.66.16	TLSv1	123	Application Data
147	6.841822000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [ACK] Seq=461 Ack=629 win=64000 Len=0
148	6.853880000	173.194.66.16	192.168.1.89	TLSv1	120	Application Data
149	6.854532000	192.168.1.89	173.194.66.16	TLSv1	111	Application Data
152	6.920651000	173.194.66.16	192.168.1.89	TLSv1	120	Application Data
153	6.921322000	192.168.1.89	173.194.66.16	TLSv1	85	Application Data
156	7.015233000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [ACK] Seq=593 Ack=717 win=64000 Len=0
163	7.399372000	173.194.66.16	192.168.1.89	TLSv1	121	Application Data
164	7.400320000	192.168.1.89	173.194.66.16	TLSv1	476	Application Data
167	7.458295000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [ACK] Seq=660 Ack=1139 win=64128 Len=0
179	8.145787000	173.194.66.16	192.168.1.89	TLSv1	131	Application Data
180	8.146948000	192.168.1.89	173.194.66.16	TLSv1	85	Application Data
184	8.200640000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [ACK] Seq=737 Ack=1170 win=64128 Len=0
185	8.212462000	173.194.66.16	192.168.1.89	TLSv1	136	Application Data
186	8.212915000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [FIN, ACK] Seq=819 Ack=1170 win=64128 Len=0
187	8.213035000	192.168.1.89	173.194.66.16	TCP	54	iax > urd [ACK] Seq=1170 Ack=820 win=64960 Len=0
188	8.220823000	192.168.1.89	173.194.66.16	TLSv1	87	Application Data
189	8.221140000	192.168.1.89	173.194.66.16	TLSv1	81	Encrypted Alert
190	8.221176000	192.168.1.89	173.194.66.16	TCP	54	iax > urd [FIN, ACK] Seq=1197 Ack=820 win=64960 Len=0
191	8.273440000	173.194.66.16	192.168.1.89	TCP	60	imps > psi-ptt [ACK] Seq=1 Ack=34 win=1002 Len=0
192	8.275693000	173.194.66.16	192.168.1.89	TCP	60	urd > iax [RST] Seq=820 win=0 Len=0
196	8.393496000	173.194.66.16	192.168.1.89	TLSv1	96	Application Data
197	8.393935000	192.168.1.89	173.194.66.16	TLSv1	93	Application Data
200	8.447002000	173.194.66.16	192.168.1.89	TCP	60	imps > psi-ptt [ACK] Seq=43 Ack=73 win=1002 Len=0
202	8.557625000	173.194.66.16	192.168.1.89	TLSv1	88	Application Data
203	8.558296000	192.168.1.89	173.194.66.16	TLSv1	122	Application Data
204	8.559395000	192.168.1.89	173.194.66.16	TLSv1	87	Application Data
205	8.611558000	173.194.66.16	192.168.1.89	TCP	60	imps > psi-ptt [ACK] Seq=77 Ack=141 win=1002 Len=0
206	8.612227000	173.194.66.16	192.168.1.89	TCP	60	imps > psi-ptt [ACK] Seq=77 Ack=174 win=1002 Len=0
219	8.975035000	173.194.66.16	192.168.1.89	TLSv1	100	Application Data
220	8.975728000	192.168.1.89	173.194.66.16	TLSv1	89	Application Data

Sposób szyfrowania wybrany w thunderbirdzie to TLS/SSL, pokazane pakiety zostały wypisane w momencie wysłania maila i są one wymianą między moim komputerem, a serwerem o ip 173.194.66.16. Polecenie whois wykazało, że jest to serwer google.

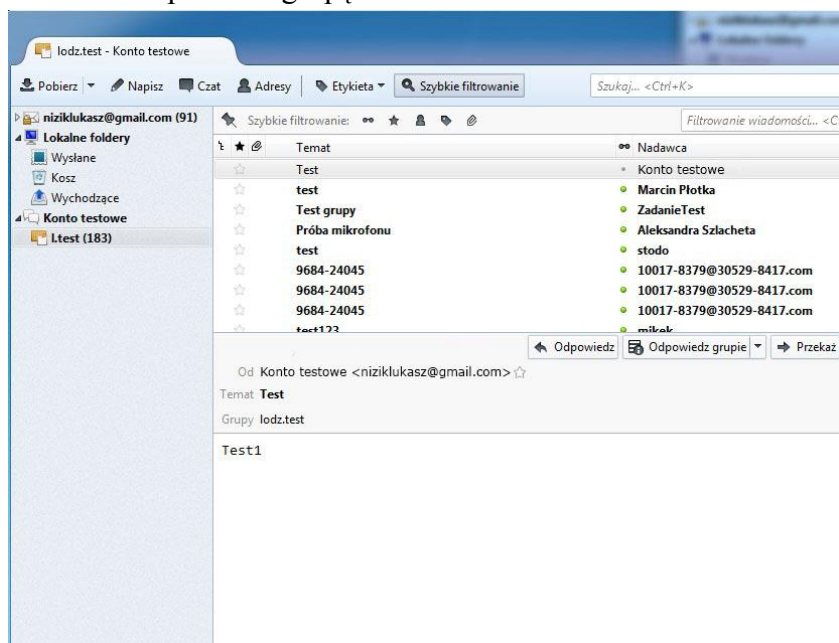
6. Skonfigurować program Thunderbird do pracy z systemem NNTP news.man.lodz.pl i przetestować jego działanie

Aby skonfigurować NNTP w programie Thunderbird należy stworzyć nową konfigurację konta dla grup dyskusyjnych. Tam podać nazwę, której chcemy używać oraz e-mail, następnie adres serwera NNTP (tu news.man.lodz.pl) i nazwę dla konta na serwerze. Żeby korzystać z konkretnej grupy dyskusyjnej należy jeszcze subskrybować ją na stworzonym przed chwilą koncie (konfiguracji).

Przeglądanie zawartości serwera NNTP:



Wstawienie posta na grupę usenet NNTP:



NNTP jest łatwym sposobem do rozpowszechniania informacji między wieloma użytkownikami, może być wykorzystany dla grup dyskusyjnych, a także ogłoszeń, wiadomości itp.