

Pytanie 1: Co to są protokoły szyfrowania wykorzystywane w transakcjach sieciowych?

Protokoły szyfrowania wykorzystywane w transakcjach sieciowych to zestawy reguł i metod szyfrowania zapewniające bezpieczną wymianę danych między komputerami i serwerami w sieci.

Pytanie 2: Wymień dwie spośród tych nazw.

Chambers of Commerce Root – 2008

EC-ACC

Pytanie 3: Pobrać zrzut ekranu z certyfikatem i wkleić go do listy odpowiedzi.

TunTrust Root CA	
Nazwa podmiotu	
Państwo	TN
Organizacja	Agence Nationale de Certification Electronique
Nazwa pospolita	TunTrust Root CA
Nazwa wystawcy	
Państwo	TN
Organizacja	Agence Nationale de Certification Electronique
Nazwa pospolita	TunTrust Root CA
Ważność	
Nieważny przed	Fri, 26 Apr 2019 08:57:56 GMT
Nieważny po	Tue, 26 Apr 2044 08:57:56 GMT
Informacje o kluczu publicznym	
Algorytm	RSA
Rozmiar klucza	4096
Wykładnik	65537
Modulo	C3:CD:D3:FC:BD:04:53:DD:0C:20:3A:D5:88:2E:05:4B:41:F5:83:82:7E:F7:59:9F...
Różne	
Numer seryjny	13:02:D5:E2:40:4C:92:46:86:16:67:5D:B4:BB:BB:B2:6B:3E:FC:13
Algorytm podpisu	SHA-256 with RSA Encryption
Wersja	3
Pobierz	PEM (certyfikat) PEM (łańcuch)
Odciski	
SHA-256	2E:44:10:2A:B5:8C:B8:54:19:45:1C:8E:19:D9:AC:F3:66:2C:AF:BC:61:4B:6A:53...
SHA-1	CF:E9:70:84:0F:E0:73:0F:9D:F6:0C:7F:2C:4B:EE:20:46:34:9C:BB
Podstawowe ograniczenia	
Organ certyfikacji	Tak

Modulo	C3:CD:D3:FC:BD:04:53:DD:0C:20:3A:D5:88:2E:05:4B:41:F5:83:82:7E:F7:59:9F...
Różne	
Numer seryjny	13:02:D5:E2:40:4C:92:46:86:16:67:5D:B4:BB:BB:B2:6B:3E:FC:13
Algorytm podpisu	SHA-256 with RSA Encryption
Wersja	3
Pobierz	PEM (certyfikat) PEM (łańcuch)
Odciski	
SHA-256	2E:44:10:2A:B5:8C:B8:54:19:45:1C:8E:19:D9:AC:F3:66:2C:AF:BC:61:4B:6A:53...
SHA-1	CF:E9:70:84:0F:E0:73:0F:9D:F6:0C:7F:2C:4B:EE:20:46:34:9C:BB
❗ Podstawowe ograniczenia	
Organ certyfikacji	Tak
❗ Zastosowania klucza	
Zastosowania	Certificate Signing, CRL Signing
Identyfikator klucza podmiotu	
Identyfikator klucza	06:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21
Identyfikator klucza organu	
Identyfikator klucza	06:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21

Pytanie 4: Jaki algorytm wykorzystano w tym przypadku?

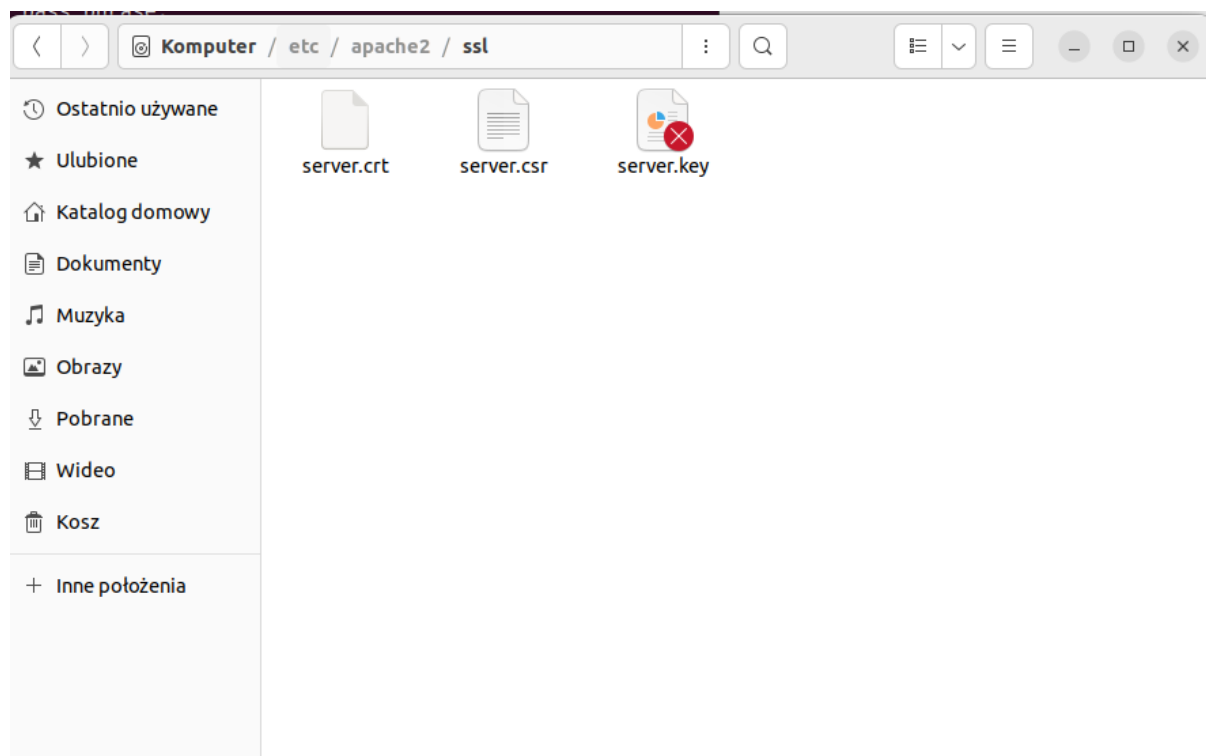
SHA-256

Pytanie 5: Jaka jest długość tego klucza w bitach?

256

Pytanie 6: Z jakich powodów certyfikat może być nieważny?

Upłynęła data ważności certyfikatu.



ubuntu-22.04.1-desktop-amd64 (zawszeOddaje) [Uruchomiona] - Oracle VirtualBox

Plik Maszyna Widok Węście Urządzenia Pomoc

Podgląd Edytor tekstu 29 paź 22:05

Otwórz [Tylko do odczytu] /etc/apache2/sites-available

Zapisz

```
1<VirtualHost *:443>
2# The ServerName directive sets the request scheme, hostname and port that
3# the server uses to identify itself. This is used when creating
4# redirection URLs. In the context of virtual hosts, the ServerName
5# specifies what hostname must appear in the request's Host: header to
6# match this virtual host. For the default virtual host (this file) this
7# value is not decisive as it is used as a last resort host regardless.
8# However, you must set it for any further virtual host explicitly.
9#ServerName www.example.com
10
11ServerAdmin webmaster@localhost
12ServerName www.testpage.net
13DocumentRoot /var/www/testpage
14
15#Pozdrawiam Filip Kazmierczak ;)
16# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
17# error, crit, alert, emerg.
18# It is also possible to configure the loglevel for particular
19# modules, e.g.
20#LogLevel info ssl:warn
21
22ErrorLog ${APACHE_LOG_DIR}/error.log
23SSLEngine On
24SSLCertificateFile /etc/apache2/ssl/server.crt
25SSLCertificateKeyFile /etc/apache2/ssl/server.key
26CustomLog ${APACHE_LOG_DIR}/access.log combined
27
28# For most configuration files from conf-available/, which are
29# enabled or disabled at a global level, it is possible to
30# include a line for only one particular virtual host. For example the
31# following line enables the CGI configuration for this host only
32# after it has been globally disabled with "a2disconf".
33#Include conf-available/serve-cgi-bin.conf
34</VirtualHost>
35
36# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Zwykły tekst Szerokość tabulacji: 4 Wrsz 15, kol 37 WST

```

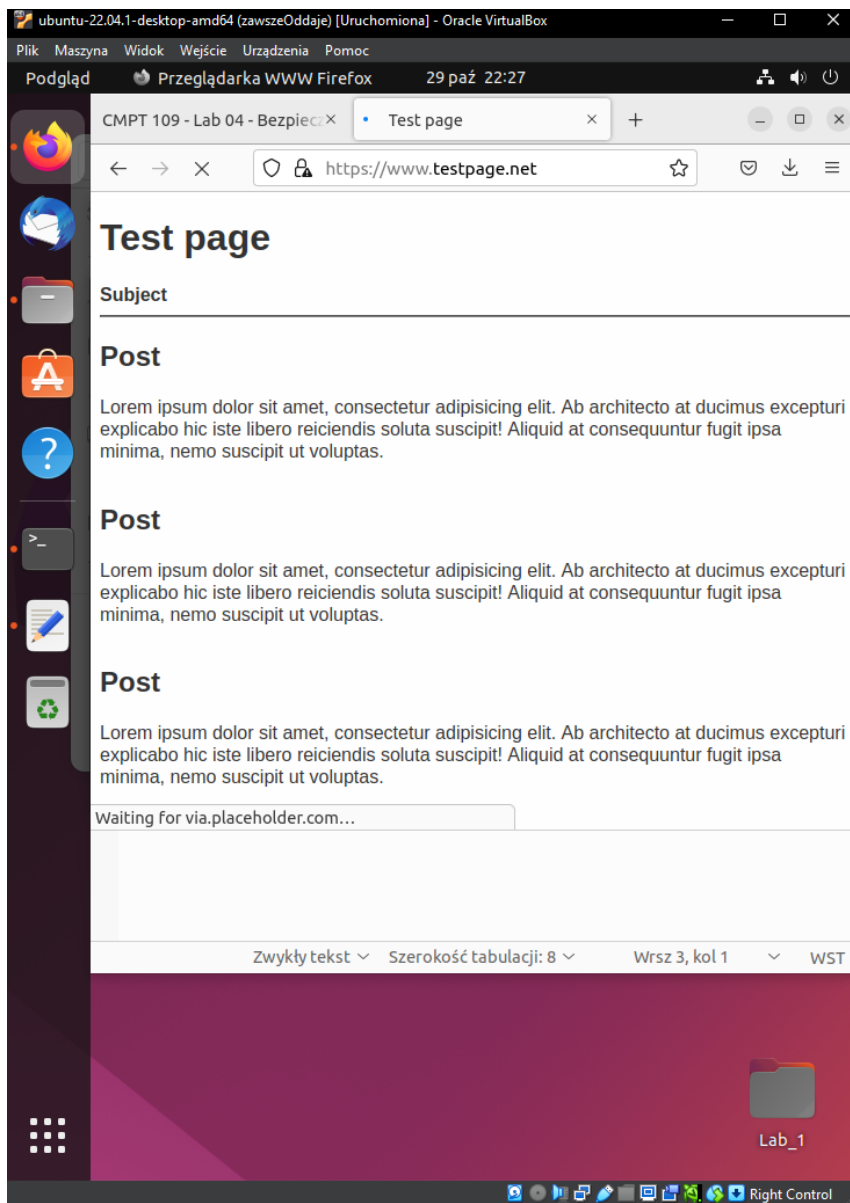
u-desktop:~$ cat /etc/hosts
1 127.0.0.1    localhost
2 127.0.1.1    ubuntu-desktop
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1          ip6-localhost ip6-loopback
6 fe00::0      ip6-localnet
7 ff00::0      ip6-mcastprefix
8 ff02::1      ip6-allnodes
9 ff02::2      ip6-allrouters
10 127.0.0.1    www.testpage.net

```

The image shows a Linux desktop environment with two windows. The left window is a terminal titled 'hosts [tylko do odczytu]' showing the installation of Apache2 on Ubuntu. The commands executed are:

```
user@ubuntu-desktop:~$ sudo apt install -y apache2
user@ubuntu-desktop:~$ sudo systemctl restart apache2
user@ubuntu-desktop:~$ curl -I http://127.0.0.1/
```

 The output shows the package being installed and the service restarted. The right window is a web browser showing the 'Apache2 Default Page' with the Ubuntu logo and the text 'it works!'. Below the logo, there is a paragraph explaining that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It mentions that the page is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. It also states that if you can read this page, it means that the Apache HTTP server installed at this site is working properly. The browser's address bar shows 'http://127.0.0.1/'.



Pytanie 7: Jaki jest okres ważności tego certyfikatu?

365 dni

Pytanie 8: Kto jest wystawcą tego certyfikatu?

Wystawcą certyfikatu jest serwer, który samodzielnie podpisuje swój certyfikat.

Pytanie 9: Jaka jest funkcja certyfikatu podczas komunikacji sieciowej między przeglądarką i Twoim serwerem WWW?

Certyfikat służy do uwierzytelniania serwera WWW, zapewniając klientowi, że połączenie jest zaufane

Podgląd Gedit 29 paź 22:36

Otwórz **handshake.txt** /home/user/Pulpit Zapisz

```
1 CONNECTED(00000003)
2 ---
3 Certificate chain
4 0 s:C = PL, ST = zachodniopomorskie, L = Szczecin, O = ZUT w
  Szczecinie, OU = ZOI WI-ZUT, CN = www.testpage.net, emailAddress =
  kfs388@zut.edu.pl
5 i:C = PL, ST = zachodniopomorskie, L = Szczecin, O = ZUT w
  Szczecinie, OU = ZOI WI-ZUT, CN = www.testpage.net, emailAddress =
  kfs388@zut.edu.pl
6 a:PKKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
7 v:NotBefore: Oct 29 20:55:31 2024 GMT; NotAfter: Oct 29 20:55:31
  2025 GMT
8 ---
9 Server certificate
10 -----BEGIN CERTIFICATE-----
11 MIID3TCCAsUCFFULGQ2IA6/0pFGApvM/0BMYbcyqMA0GCSqGSIb3DQEBQwAMIGQ
12 M0swCOYDVQGEWJQDEBMBKA1UECAwSemFjaG9kbmlvcG9tb3Jza2l1MREwDwYD
13 VQ0HDAHTemN6ZWNPbjEZMBcGA1UECgwWVUIHcgU3pjemVjaW5pZTETMBEGA1UE
14 CwwKwK9JIFdJLpVpVDEZMBcGA1UEAwQd3d3LnRlc3RwYXd1Lm5ldDEgMB4GCSqG
15 SIb3DQEJARYRa2Y1Mzg4QHp1dC5LZHUucGwwHhcnMjQxMDI5MjA1NTMxWhcnMjUx
16 MDI5MjA1NTMxWjCBajELMAKGA1UEBhMCUEwGZAZBgNVBAQMEPhY2hvZG5pb3Bv
17 bW9yc2tpZTERMA8GA1UEBwwU3pjemVjaW4xGTAxBGNVBAQMEPhY2hvZG5pb3Bv
18 Y2L1uaWUxEzARBgNVBAsMClpSSSB5S1aVWQxGTAxBGNVBAQMEHd3dy50ZXN0cGFn
19 ZS5uZXQxIDAeBgkqhkiG9w0BCEWEWtmNTM4OE6dXQuZWR1LnBsMIIIBjANBgkq
20 hkiG9w0BAQEFAAOCAQAMIBCBQCAQEAQAc0xHYooAF+vCatJL+YdJPH0grCKnLC
21 QHzfKmpPV3zrL/GRXVcLLK0YVv0hm2oPgICENDoyH158Rh3020M0gXSeBMzyTOVE
22 PTKWmTv5/72XZofk+9uS5yqCboupKygIeXfymitQZWh90wA9hdm9AqzbrUQQds
23 08BKehw63kAE4tJ7d3QCDvr5/WrK3A0b/q00pZgZrNzdinPkqU/69xC94u+dZeif
24 0nrBf09YfyzLxw5d/2HzdUJXB6CUES0m+NwpUJ/24sTz1njq0YVqvUHLI055ES
25 KGwAzm5F/SnpZP124y9zbBVFqL+bm6yJWsJT6cgrP1+omxqQGw/c3QIDAQABMA0G
26 CSqGSIb3DQEBQwAAIA1BAQBzBTJez/giCSUjdCTRjkKFH+6GcCeB0CUT/+lgsop
27 a2LWLf++JcywX680N0B4CtbgdGZANfXzrzZt0QY2xPXPak9Co4bz7Egcj2/9Nd
28 +GniPyyp0PhNRu0fa2JTotPvd9AlFajTKdDfqnLORP677U7imeGyHkSF3PhVel58
29 SyuEYo2Jhu94YQzsgm/wCyZ38jxLHK/G80en/PJmQldpZBF5Uf1yB9DreN44jbBs
30 90atqfSMe3+iuSadX2s9rrcVDP9nAX+/cB931gNzX/UrD7i0EsLMTN0/JZuM2U8e
31 B35cCb6zyA/ZX+Hw5eSRXoy08L+Rae+42NH8L02VxI1y
32 -----END CERTIFICATE-----
```

Zwyczajny tekst Szerokość tabulacji: 8 Wiersz 1, kol 1 WST

handshake.txt

Plik C:/Users/piotr/Downloads... 15 z 15

Pytanie 10: Dlaczego serwer WWW wysłał jakiegokolwiek informację?

Pytanie 11: Jakie informacje zawiera plik *handshake.txt*?

4. Zamknij edytor tekstowy "gedit", terminal i wirtualną maszynę Ubuntu.

Sprawozdanie z ćwiczenia

W trakcie ćwiczenia należy notować wszystkie czynności oraz uzyskiwane wyniki. Po zakończeniu ćwiczenia należy przygotować sprawozdanie z przebiegu ćwiczenia, zawierające m.in. krótki opis ćwiczenia, uzyskane wyniki oraz podsumowanie i wnioski z ćwiczenia. Sprawozdanie powinno zawierać także odpowiedzi na wszystkie pytania zadane w konspekcie.

Pytanie 10: Dlaczego serwer WWW wysłał jakiegokolwiek informację?

Serwer WWW wysłał informację, aby odpowiedzieć na żądanie klienta, który chce ustanowić bezpieczne połączenie.

Pytanie 11: Jakie informacje zawiera plik *handshake.txt*?

Zawiera szczegóły związane z procesem negocjacji SSL, w tym informacje na temat certyfikatu serwera i parametrów szyfrowania.