DIGICERT® CERTIFICATION PROGRAM

DigiCert Technical Certifications SSL/TLS Professional Training Guide

Introduction

This training guide is designed to help you prepare for the **DigiCert Technical Certification: SSL/TLS Professional** assessment exam. The exam will consist of 50 multiple-choice questions with a maximum time allowed of 1 hour.

The intended audience for this assessment is anybody who works with SSL/TLS technology in a technical role (technical support, SSL/TLS administrator, etc).

Objectives

Before attempting the **DigiCert Technical Certification: SSL/TLS Professional** assessment exam, you should be able to do the following:

- Describe the main purpose and functions of SSL & TLS
- Describe the history and versions of SSL & TLS
- Describe symmetric and asymmetric encryption models
- Describe how digital signatures work
- Describe the details of an SSL/TLS certificate, including extensions and file formats
- Describe DV, OV, EV and private SSL certificates
- Describe the benefits of EV certificates
- Describe SAN and wildcard certificates
- Describe domain control and organisation validation methods
- Describe how the SSL/TLS "handshake" works in detail, Including the role of root, intermediate (ICA), end-entity and cross-root certificates
- Describe the CRL and OCSP methods for revocation checking (including OCSP Stapling)

- List common algorithms used in TLS for key agreement, encryption, digital signatures, and hashing
- Describe "Forward Secrecy"
- List the benefits of Elliptic Curve Cryptography for TLS
- Explain the dangers of expired, misconfigured, self-signed and "vendor" certificates
- Identify common vulnerabilities of outdated protocols (Heartbleed, etc)
- Describe how phishing websites work
- Describe Server Name Indication (SNI)
- Describe Certificate Transparency (CT)
- Describe Certificate Authority
 Authorisation (CAA)
- Describe Certificate Pinning
- Describe HTTP Strict Transport Security (HSTS)
- Describe HTTP/2
- Explain the term "Always-on SSL"
- Explain the role of the CA/B Forum
- List and describe best practices for SSL security and performance

digicert

DIGICERT® CERTIFICATION PROGRAM

- Describe the ACME protocol
- Describe Google AMP (Accelerated Mobile Pages), Signed HTTP Exchange (SXG) and delegated credentials
- Describe commonly-used SSL/TLS CSR generation and certificate tools, e.g. OpenSSL, Java Keystore

Training Guide

Before attempting a certification assessment, you should review the objectives above.

If you believe that you are already able to meet all the objectives listed, you are welcome to schedule an assessment. However, if there are any objectives listed where you may need additional preparation, you should plan to research these topics in detail prior to scheduling an assessment.

Below you will find links for e-learning, downloads and relevant websites. Please note – these resources are just a starting point! It is strongly recommended that you do further research in order to be fully prepared for an assessment on all the objectives. This could include research on the internet (e.g. Wikipedia) and/or hands-on experience using relevant DigiCert products and tools.

In addition to the self-directed learning options described above, it may be possible to attend a DigiCert instructor-based workshop which will give in-depth information on many of the assessment objectives. Please contact your DigiCert account manager if you would like to find out more.

Recommended Self-paced Training

Training Videos SSL/TLS Fundamentals (0:52) SSL/TLS Deep-Dive (0:45) SSL/TLS Risks and Vulnerabilities (0:27) SSL/TLS Industry Trends (0:38)	https://vimeo.com/showcase/8411250 https://m.youtube.com/user/digicertssl
SSL Best Practice Workshop Student Guide	https://www.digicert.com/digicert-tls-ssl-certified-
	expert/#downloads
NIST SP 1800-16: Securing Web Transactions:	https://csrc.nist.gov/publications/detail/sp/1800-
TLS Server Certificate Management	<u>16/final</u>
TLS Best Practice eBook	https://www.digicert.com/resources/tls-best-
	practices.pdf
SSL/TLS and PKI History	https://www.feistyduck.com/ssl-tls-and-pki-
	history/

available in multiple languages

DIGICERT® CERTIFICATION PROGRAM

Additional Resources

CA/Browser Forum Baseline https://cabforum.org/baseline-requirements-documents/ Requirements		
CA/Browser Forum Guidelines for EV Certificates https://cabforum.org/extended-validation/ TLS 1.2 (RFC 5246) https://tools.ietf.org/html/rfc5246 TLS 1.3 (RFC 8446) https://tools.ietf.org/html/rfc5446 OCSP (RFC 6960) https://tools.ietf.org/html/rfc6960 SNI (RFC 6066) https://tools.ietf.org/html/rfc6066#section-3 CAA (RFC 6844) https://tools.ietf.org/html/rfc6797 HSTS (RFC 6797) https://tools.ietf.org/html/rfc6797 HTTP/2 (RFC 7540) https://tools.ietf.org/html/rfc6797 ACME (RFC 8555) https://tools.ietf.org/html/rfc540 ACME (RFC 8555) https://tools.ietf.org/html/rfc8445 Delegated Credentials https://tools.ietf.org/html/rfc8445 Certificate Transparency https://tols.ietf.org/html/rfc8445 US Government Compliance https://tols.ietf.org/html/rfc8445 "Always-on" SSL https://totalliance.org/resources/always-ssl-aossl https://tot	CA/Browser Forum Baseline	https://cabforum.org/baseline-requirements-documents/
for EV CertificatesTLS 1.2 (RFC 5246)https://tools.ietf.org/html/rfc5246TLS 1.3 (RFC 8446)https://tools.ietf.org/html/rfc8446OCSP (RFC 6960)https://tools.ietf.org/html/rfc6960SNI (RFC 6066)https://tools.ietf.org/html/rfc6066#section-3CAA (RFC 6844)https://tools.ietf.org/html/rfc6844https://tools.ietf.org/html/rfc6797HTTP/2 (RFC 7540)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555AMP & SXGhttps://www.digicert.com/google-amp-security-solutions/ https://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://blog.cloudflare.com/keyless-delegation/US Government Compliancehttps://totalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://casecurity.org/2016/09/30/always-on-ssl/ 		
TLS 1.2 (RFC 5246)https://tools.ietf.org/html/rfc5246TLS 1.3 (RFC 8446)https://tools.ietf.org/html/rfc6446OCSP (RFC 6960)https://tools.ietf.org/html/rfc6960SNI (RFC 6066)https://tools.ietf.org/html/rfc6066#section-3CAA (RFC 6844)https://tools.ietf.org/html/rfc6844https://tools.ietf.org/html/rfc6797HTSS (RFC 6797)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555Ocentralishttps://tools.ietf.org/html/rfc8555Ocentralishttps://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555Oelegated Credentialshttps://tools.ietf.org/ktml/rfc8555Oesorement Compliancehttps://log.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://lotalliance.org/resources/always-ssl-aosslhttps://claalliance.org/resources/always-on-ssl./https://claalliance.org/resources/always-on-ssl./Mttps://www.digicert.com/looks/openssl-cookbook/https://www.digicert.com/sol-cordialways-on-ssl./Mttps://www.digicert.com/sol-certificate-installation.htmcertificate-installation.htm	CA/Browser Forum Guidelines	https://cabforum.org/extended-validation/
TLS 1.3 (RFC 8446)https://tools.ietf.org/html/rfc8446OCSP (RFC 6960)https://tools.ietf.org/html/rfc6960SNI (RFC 6066)https://tools.ietf.org/html/rfc6066#section-3CAA (RFC 6844)https://tools.ietf.org/html/rfc6844https://tools.ietf.org/html/rfc6797HSTS (RFC 6797)https://tools.ietf.org/html/rfc790HTTP/2 (RFC 7540)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555Oelegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://tools.ietf.org/nguide/#compliance-and-best-practice- guideGuidehttps://totalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.digicert.com/sol-cookbook/General CSR Creationhttps://www.digicert.com/ssl-certificate-installation.htmGuidelineshttps://www.digicert.com/ssl-certificate-installation.htm	for EV Certificates	
OCSP (RFC 6960)https://tools.ietf.org/html/rfc6960SNI (RFC 6066)https://tools.ietf.org/html/rfc6066#section-3CAA (RFC 6844)https://tools.ietf.org/html/rfc6844https://www.digicert.com/blog/new-caa-requirement-2/HSTS (RFC 6797)https://tools.ietf.org/html/rfc6797HTTP/2 (RFC 7540)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555AMP & SXGhttps://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://www.certificate-transparency.org/US Government Compliance Guidehttps://totalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.digicert.com/sol-certificate-installation.htmGeneral CSR Creation Guidelineshttps://www.digicert.com/ssl-certificate-installation.htm	TLS 1.2 (RFC 5246)	https://tools.ietf.org/html/rfc5246
SNI (RFC 6066) https://tools.ietf.org/html/rfc6066#section-3 CAA (RFC 6844) https://tools.ietf.org/html/rfc6844 https://www.digicert.com/blog/new-caa-requirement-2/ HSTS (RFC 6797) https://tools.ietf.org/html/rfc6797 HTTP/2 (RFC 7540) https://tools.ietf.org/html/rfc7540 ACME (RFC 8555) https://tools.ietf.org/html/rfc8555 AMP & SXG https://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/ Delegated Credentials https://blog.cloudflare.com/keyless-delegation/ Certificate Transparency https://https.cio.gov/guide/#compliance-and-best-practice- checklist "Always-on" SSL https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl/ https://www.digicert.com/sol-coskbook/ General CSR Creation https://www.digicert.com/csr-creation.htm Guidelines https://www.digicert.com/ssl-certificate-installation.htm How to Install an SSL Certificate https://www.digicert.com/ssl-certificate-installation.htm	TLS 1.3 (RFC 8446)	https://tools.ietf.org/html/rfc8446
CAA (RFC 6844)https://tools.ietf.org/html/rfc6844 https://tools.ietf.org/html/rfc6797HSTS (RFC 6797)https://tools.ietf.org/html/rfc6797HTTP/2 (RFC 7540)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://tools.ietf.org/html/rfc8555Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://www.certificate-transparency.org/US Government Compliancehttps://totaliance.org/resources/always-ssl-aosslMttps://otaliance.org/resources/always-on-ssl/ https://www.digicert.com/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.digicert.com/soks/openssl-cookbook/How to Install an SSL Certificatehttps://www.digicert.com/ssl-certificate-installation.htm	OCSP (RFC 6960)	https://tools.ietf.org/html/rfc6960
https://www.digicert.com/blog/new-caa-requirement-2/HSTS (RFC 6797)https://tools.ietf.org/html/rfc6797HTTP/2 (RFC 7540)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://www.certificate-transparency.org/US Government Compliancehttps://ttps.cio.gov/guide/#compliance-and-best-practice- checklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aossl https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.digicert.com/sol-certificate-installation.htmGuidelineshttps://www.digicert.com/csr-creation.htmHow to Install an SSL Certificatehttps://www.digicert.com/ssl-certificate-installation.htm	SNI (RFC 6066)	https://tools.ietf.org/html/rfc6066#section-3
HSTS (RFC 6797)https://tools.ietf.org/html/rfc6797HTTP/2 (RFC 7540)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://totalliance.org/resources/always-ssl-aossl https://totalliance.org/resources/always-ssl-aossl https://www.digicert.com/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.digicert.com/ssl-certificate-installation.htm GuidelinesHow to Install an SSL Certificatehttps://www.digicert.com/ssl-certificate-installation.htm	CAA (RFC 6844)	https://tools.ietf.org/html/rfc6844
HTTP/2 (RFC 7540)https://tools.ietf.org/html/rfc7540ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://www.certificate-transparency.org/US Government Compliance Guidehttps://otalliance.org/resources/always-ssl-aossl https://otalliance.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.digicert.com/solves/openssl-cookbook/General CSR Creation Guidelineshttps://www.digicert.com/ssl-certificate-installation.htmHow to Install an SSL Certificatehttps://www.digicert.com/ssl-certificate-installation.htm		https://www.digicert.com/blog/new-caa-requirement-2/
ACME (RFC 8555)https://tools.ietf.org/html/rfc8555AMP & SXGhttps://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://www.certificate-transparency.org/US Government Compliancehttps://https.cio.gov/guide/#compliance-and-best-practice- checklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.digicert.com/sol-certificate-installation.htmGeneral CSR Creationhttps://www.digicert.com/ssl-certificate-installation.htmHow to Install an SSL Certificatehttps://www.digicert.com/ssl-certificate-installation.htm	HSTS (RFC 6797)	https://tools.ietf.org/html/rfc6797
AMP & SXGhttps://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://www.certificate-transparency.org/US Government Compliancehttps://https.cio.gov/guide/#compliance-and-best-practice- checklistGuidehttps://casecurity.org/2016/09/30/always-on-sslMttps://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.feistyduck.com/books/openssl-cookbook/General CSR Creationhttps://www.digicert.com/csr-creation.htmGuidelineshttps://www.digicert.com/csr-creation.htmHow to Install an SSLhttps://www.digicert.com/ssl-certificate-installation.htm	HTTP/2 (RFC 7540)	https://tools.ietf.org/html/rfc7540
https://www.digicert.com/blog/googles-signed-http-exchange- solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://blog.cloudflare.com/keyless-delegation/US Government Compliancehttps://https.cio.gov/guide/#compliance-and-best-practice- checklistGuidechecklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.feistyduck.com/books/openssl-cookbook/General CSR Creationhttps://www.digicert.com/csr-creation.htmHow to Install an SSLhttps://www.digicert.com/ssl-certificate-installation.htm	ACME (RFC 8555)	https://tools.ietf.org/html/rfc8555
solution-displays-publisher-urls-for-amp-pages-via-tls/Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://www.certificate-transparency.org/US Government Compliancehttps://https.cio.gov/guide/#compliance-and-best-practice-Guidechecklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aosslhttps://casecurity.org/2016/09/30/always-on-ssl/https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.orgHttps://www.feistyduck.com/books/openssl-cookbook/Https://www.digicert.com/csr-creation.htmGuidelineshttps://www.digicert.com/csr-creation.htmHow to Install an SSLhttps://www.digicert.com/ssl-certificate-installation.htm	AMP & SXG	https://www.digicert.com/google-amp-security-solutions/
Delegated Credentialshttps://blog.cloudflare.com/keyless-delegation/Certificate Transparencyhttps://www.certificate-transparency.org/US Government Compliancehttps://https.cio.gov/guide/#compliance-and-best-practice-Guidechecklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aosslhttps://casecurity.org/2016/09/30/always-on-ssl/https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.orgGeneral CSR Creationhttps://www.digicert.com/csr-creation.htmGuidelineshttps://www.digicert.com/csr-creation.htmHow to Install an SSLhttps://www.digicert.com/ssl-certificate-installation.htm		https://www.digicert.com/blog/googles-signed-http-exchange-
Certificate Transparencyhttps://www.certificate-transparency.org/US Government Compliancehttps://https.cio.gov/guide/#compliance-and-best-practice- checklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.feistyduck.com/books/openssl-cookbook/General CSR Creationhttps://www.digicert.com/csr-creation.htmGuidelineshttps://www.digicert.com/ssl-certificate-installation.htm		solution-displays-publisher-urls-for-amp-pages-via-tls/
US Government Compliancehttps://https.cio.gov/guide/#compliance-and-best-practice- checklistGuidechecklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.feistyduck.com/books/openssl-cookbook/General CSR Creation Guidelineshttps://www.digicert.com/csr-creation.htmHow to Install an SSL Certificatehttps://www.digicert.com/ssl-certificate-installation.htm	Delegated Credentials	https://blog.cloudflare.com/keyless-delegation/
Guidechecklist"Always-on" SSLhttps://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htmOpenSSLwww.openssl.org https://www.feistyduck.com/books/openssl-cookbook/General CSR Creation Guidelineshttps://www.digicert.com/csr-creation.htm GuidelinesHow to Install an SSL Certificatehttps://www.digicert.com/ssl-certificate-installation.htm	Certificate Transparency	https://www.certificate-transparency.org/
"Always-on" SSL https://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htm OpenSSL www.openssl.org https://www.feistyduck.com/books/openssl-cookbook/ General CSR Creation https://www.digicert.com/csr-creation.htm Guidelines https://www.digicert.com/csr-creation.htm How to Install an SSL https://www.digicert.com/ssl-certificate-installation.htm	US Government Compliance	https://https.cio.gov/guide/#compliance-and-best-practice-
https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htm OpenSSL www.openssl.org https://www.feistyduck.com/books/openssl-cookbook/ General CSR Creation https://www.digicert.com/csr-creation.htm Guidelines https://www.digicert.com/ssl-certificate-installation.htm How to Install an SSL https://www.digicert.com/ssl-certificate-installation.htm	Guide	<u>checklist</u>
https://www.digicert.com/always-on-ssl.htm OpenSSL www.openssl.org https://www.feistyduck.com/books/openssl-cookbook/ General CSR Creation Guidelines https://www.digicert.com/csr-creation.htm How to Install an SSL Certificate https://www.digicert.com/ssl-certificate-installation.htm	"Always-on" SSL	https://otalliance.org/resources/always-ssl-aossl
OpenSSL www.openssl.org https://www.feistyduck.com/books/openssl-cookbook/ General CSR Creation https://www.digicert.com/csr-creation.htm Guidelines https://www.digicert.com/csr-creation.htm How to Install an SSL https://www.digicert.com/ssl-certificate-installation.htm Certificate opensed		https://casecurity.org/2016/09/30/always-on-ssl/
https://www.feistyduck.com/books/openssl-cookbook/ General CSR Creation https://www.digicert.com/csr-creation.htm Guidelines https://www.digicert.com/csr-creation.htm How to Install an SSL https://www.digicert.com/ssl-certificate-installation.htm Certificate certificate		https://www.digicert.com/always-on-ssl.htm
General CSR Creation https://www.digicert.com/csr-creation.htm Guidelines https://www.digicert.com/ssl-certificate-installation.htm How to Install an SSL https://www.digicert.com/ssl-certificate-installation.htm Certificate certificate	OpenSSL	www.openssl.org
Guidelines How to Install an SSL Certificate Certificate		https://www.feistyduck.com/books/openssl-cookbook/
How to Install an SSL https://www.digicert.com/ssl-certificate-installation.htm Certificate	General CSR Creation	https://www.digicert.com/csr-creation.htm
Certificate	Guidelines	
	How to Install an SSL	https://www.digicert.com/ssl-certificate-installation.htm
Certificate file formats https://knowledge.digicert.com/generalinformation/INFO4448.html	Certificate	
	Certificate file formats	https://knowledge.digicert.com/generalinformation/INFO4448.html

E-learning (YouTube)

Cryptography Overview (8:31)	Cryptographic Hash Functions (7:04)
Symmetric vs. Asymmetric Encryption (4:18)	Symmetric Encryption Ciphers (6:42)
Public Keys and Private Keys (4:10)	Asymmetric Cryptography Algorithms (2:36)
Session Keys (4:22)	Certificate Authorities (2:52)
Block vs. Stream Ciphers (3:13)	Key Revocation (3:31)
Hashing (3:30)	Digital Certificates (3:01)
Perfect Forward Secrecy (3:38)	Public Key Infrastructure (3:33)