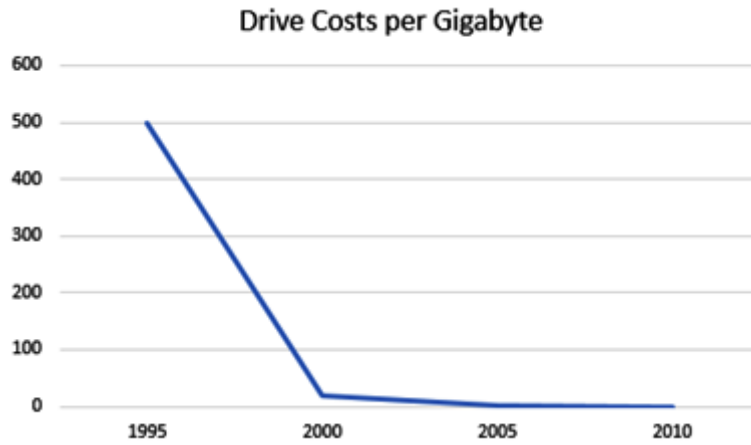


Chapter 1: Protecting Data in Motion or at Rest



FileA Baseline



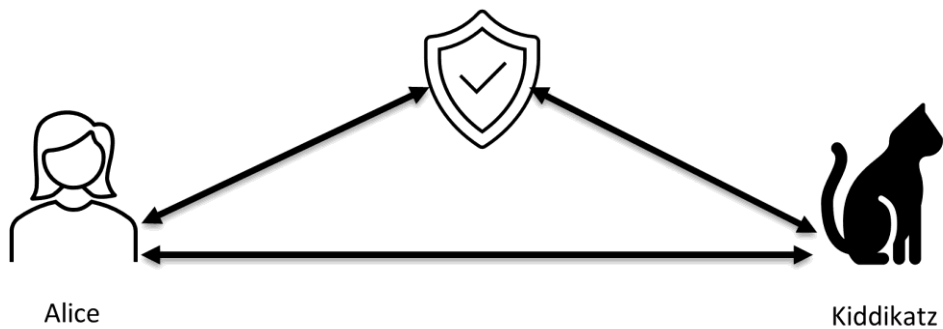
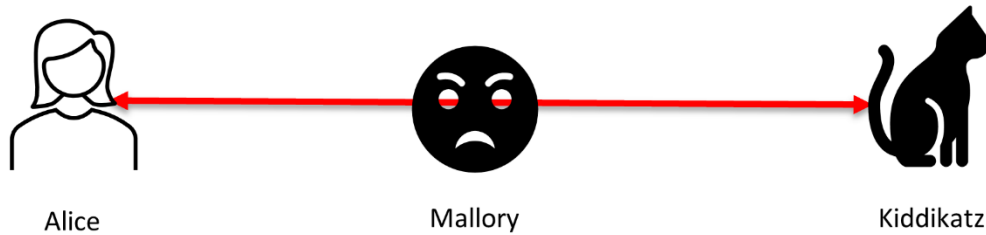
HASH
723js8oyqwy



FileA Checked



HASH
673js8oybwa

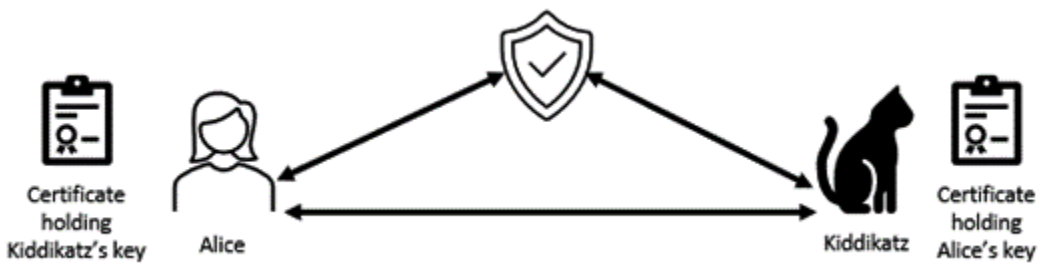


https://www.packtpub.com

Connection Security for www.packtpub.com

You are securely connected to this site.

Verified by: Cloudflare, Inc.



A	B	C	J	K	L
D	E	F	M	N	O
G	H	I	P	Q	R

S	W
T	X
V	Y
	Z

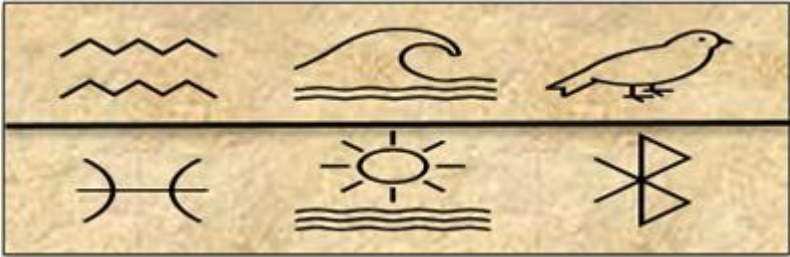
VOLF0> 30VVJ70

T	Y	I	N	S	U	P	C	E
K	R	I	N	M	P	U	S	U
K	Y	A	W	Q	Z	O	A	B

T	Y	I	N	S	U	P	C	E
K	R	I	N	M	P	U	S	U
K	Y	A	W	Q	Z	O	A	B

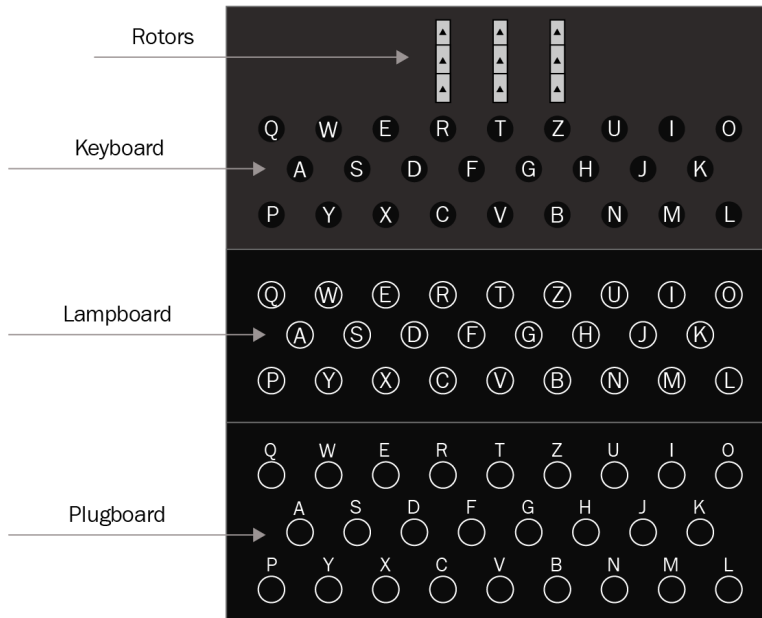
6□■7†±ℓ■◆†∞●†◆☒ †• &ℓℓ□†■7□□†❖∞◆ℓ 5∞◆∞ □
 □†❖∞◆ℓ 2☒ □□□◆ℓ 7††■7 ∞7∞†■◆ ◆■∞◆◆≡□□†℔ℓ±
 ±†•7●□◆□ℓ☒

Chapter 2: The Evolution of Ciphers



A	B	C	D	E	F	G
F	G	A	B	C	D	E

L	E	T	S	S	T	U	D	Y	C	R	Y	P	T	O	G	R	A	P	H	Y
T	I	G	E	R	K	I	T	T	E	N	S	T	I	G	E	R	K	I	T	T
E	M	Z	W	J	D	C	W	R	G	E	Q	I	B	U	K	I	K	X	A	R



43	30	55	41
23	52	30	44
41	01	45	22
9F	33	21	00

Input

HEX	y						
	0	1	2	3	4	5	
x	0	03	79	B5	A4	67	12
	1	C7	D3	52	89	FF	19
	2	32	0D	B9	16	F4	79
	3	BF	54	AA	E0	C1	DD
	4	E2	08	59	EA	63	45

S-BOX

43

	30	55	41
23	52	30	44
41	01	45	22
9F	33	21	00

Input

HEX		y					
		0	1	2	3	4	5
x	0	03	79	B5	A4	67	12
	1	C7	D3	52	89	FF	19
	2	32	0D	B9	16	F4	79
	3	BF	54	AA	E0	C1	DD
	4	E2	08	59	EA	63	45

S-BOX

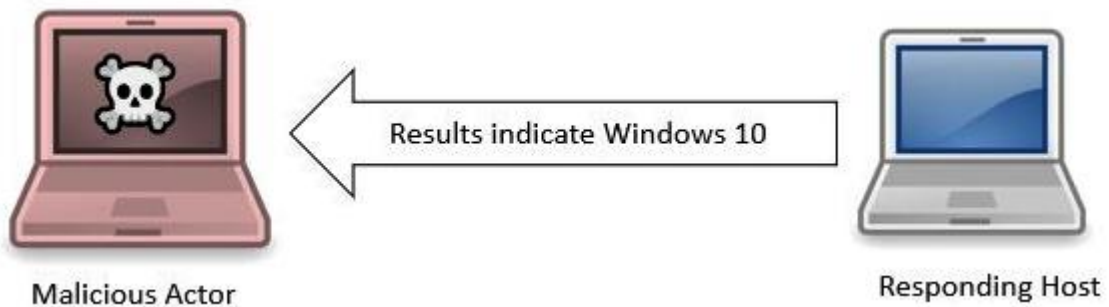
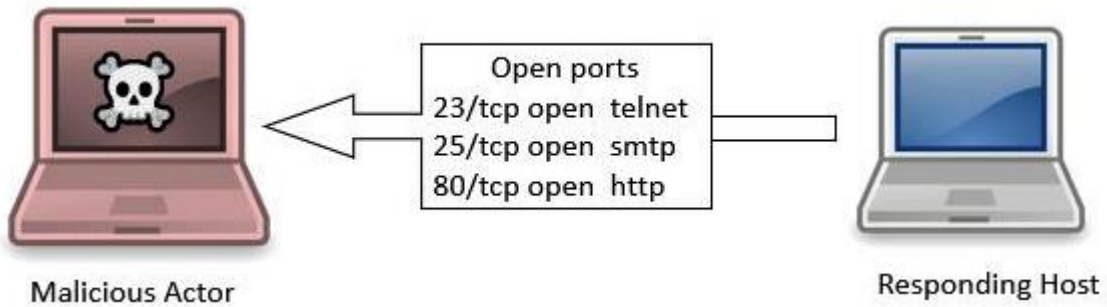
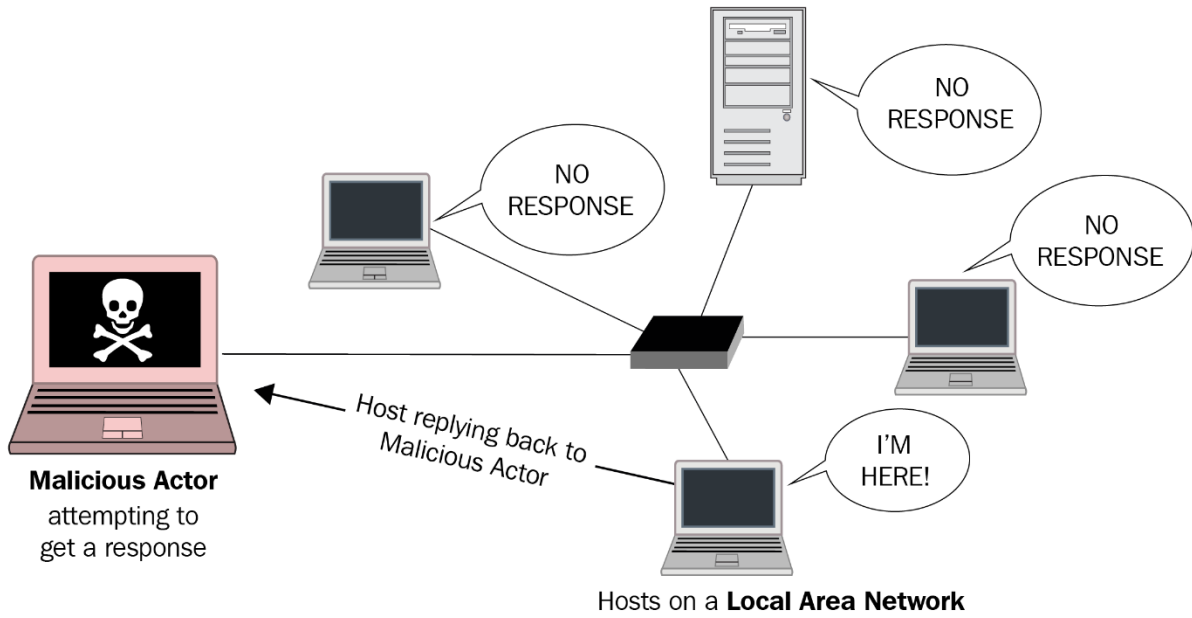
C1	30	55	41
23	52	30	44
41	01	45	22
9F	33	21	00

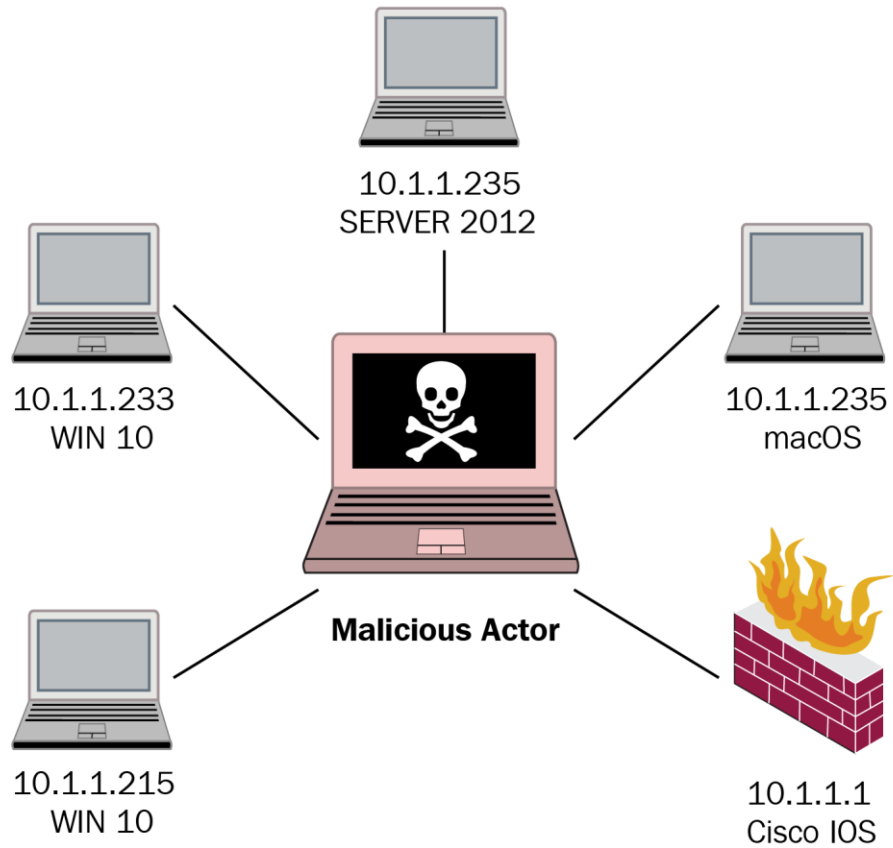
Input

HEX		y					
		0	1	2	3	4	5
x	0	03	79	B5	A4	67	12
	1	C7	D3	52	89	FF	19
	2	32	0D	B9	16	F4	79
	3	BF	54	AA	E0	C1	DD
	4	E2	08	59	EA	63	45

S-BOX

Chapter 3: Evaluating Network Attacks





```

Nmap scan report for 10.0.0.167
Host is up (0.0034s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
6839/tcp  open  unknown
7435/tcp  open  unknown
8080/tcp  open  http-proxy
8089/tcp  open  unknown
9102/tcp  open  jetdirect
9110/tcp  open  unknown
9111/tcp  open  DragonIDSConsole
9220/tcp  open  unknown
9290/tcp  open  unknown
MAC Address: 08:2E:5F:F2:32:18 (Hewlett Packard)

```

```
Cookie: PHPSESSID=7ruccrgatd7dgnp767iudh7fb6  
Upgrade-Insecure-Requests: 1
```

```
email=admin%40google.com&password=Password2010HT  
TP/1.1 302 Moved Temporarily  
Date: Fri, 29 May 2020 01:12:37 GMT  
Server: Apache  
X-Powered-By: PHP/5.6.40
```

2 client pkts, 2 server pkts, 3 turns.

Entire conversation (3489 bytes)

Show and save data as ASCII

Stream 37

Find:

Find Next

Filter Out This Stream

Print

Save as...

Back

Close

Help

Malicious Actor



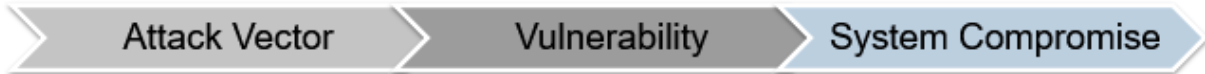
Gaining Control

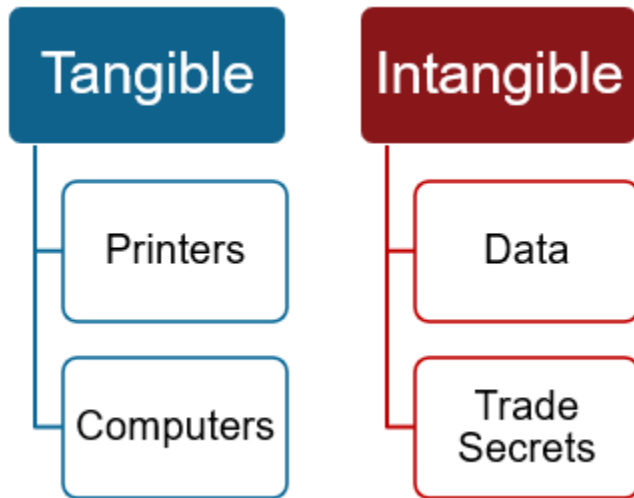
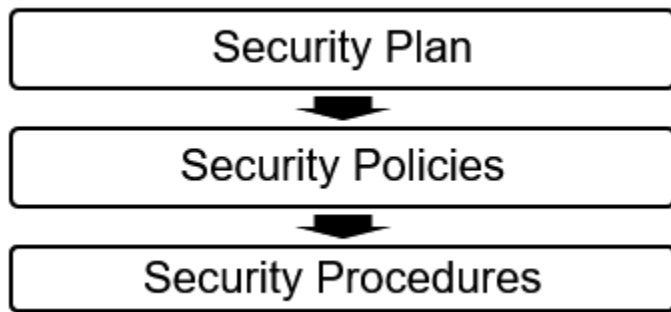
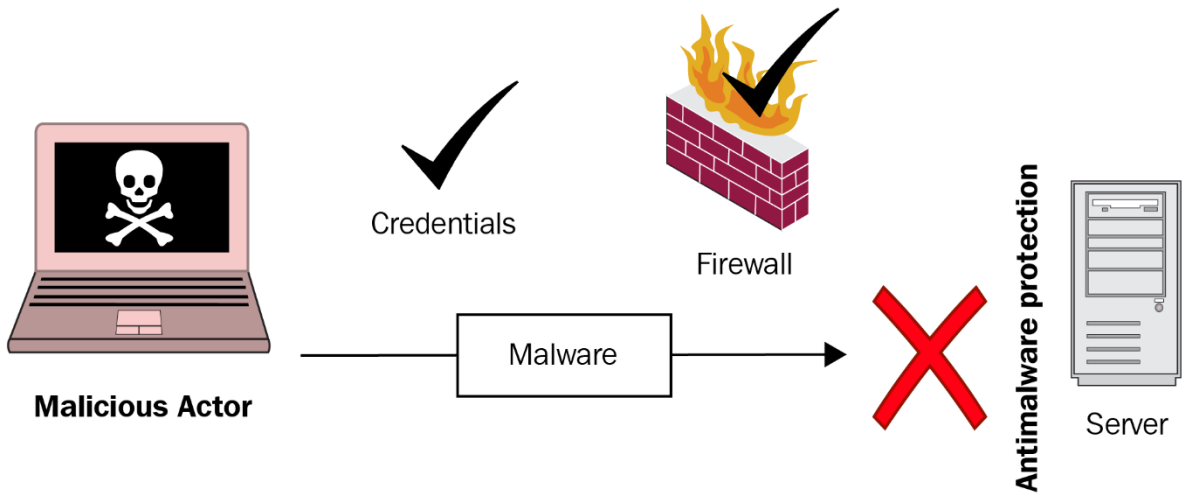


Attack Vector

Vulnerability

System Compromise

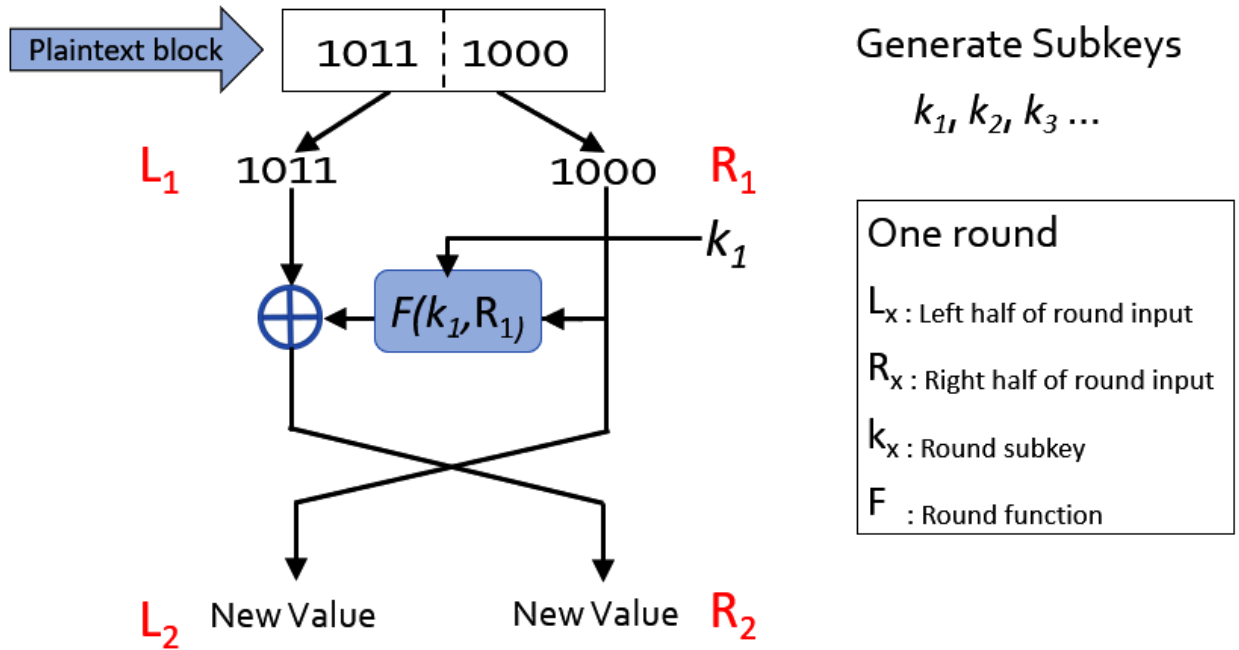




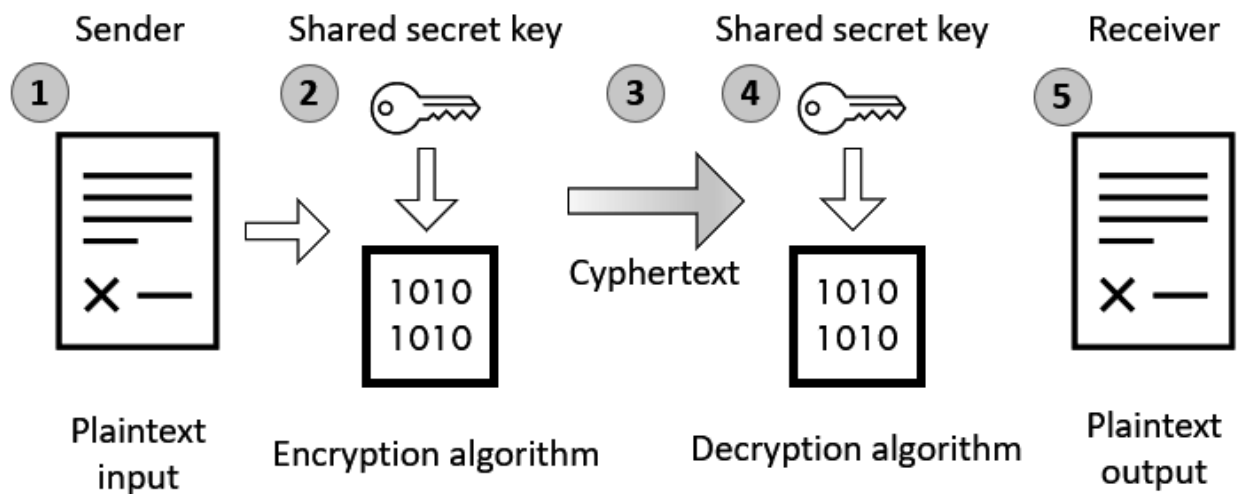
Risk = Threat \times Vulnerability

Scenario	Risk	=	Threat	X	Vulnerability
Free antivirus	90%	=	100%	X	90%
Paid antivirus	40%	=	100%	X	40%
UTM	10%	=	100%	X	10%

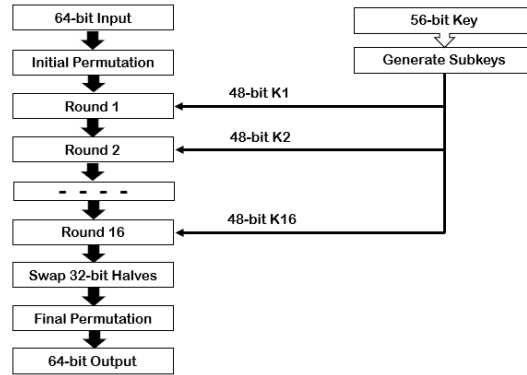
Chapter 4: Introducing Symmetric Encryption



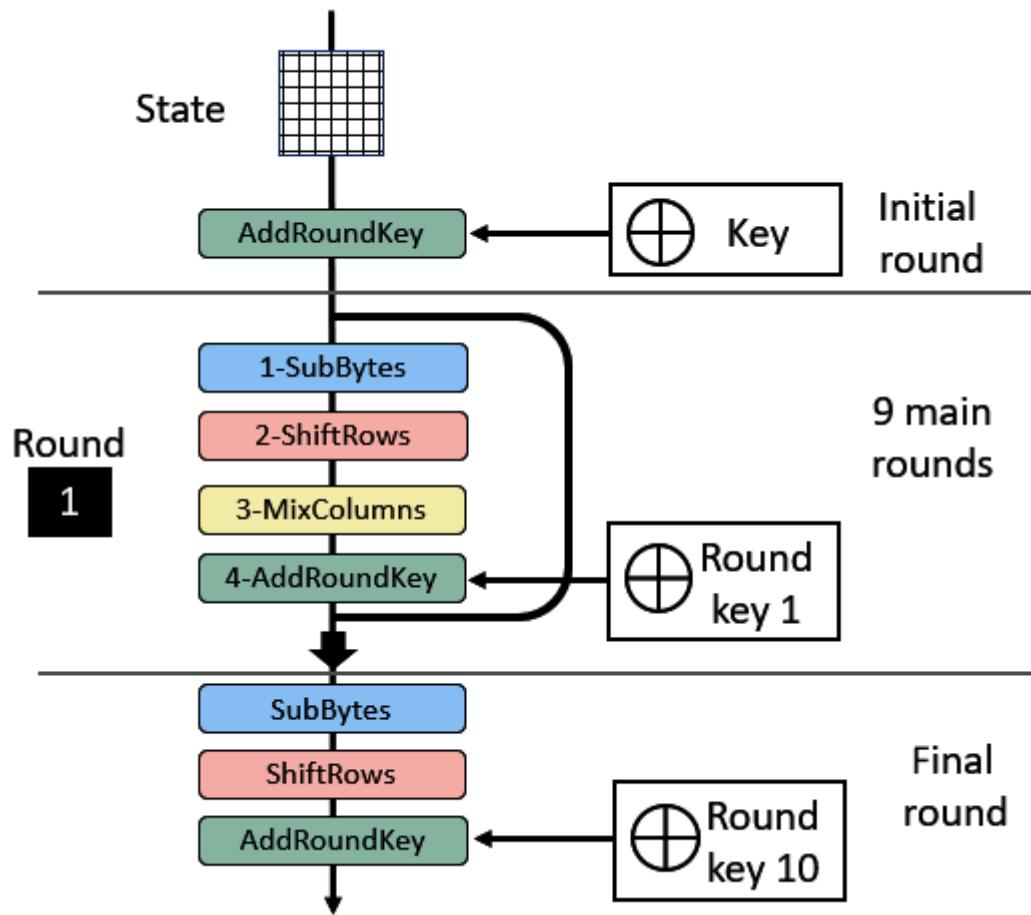
A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64



b0	b4	b8	b12	➔	43	30	55	41
b1	b5	b9	b13		23	52	3B	44
b2	b6	b10	b14		41	1C	45	22
b3	b7	b11	b15		9F	33	21	0A

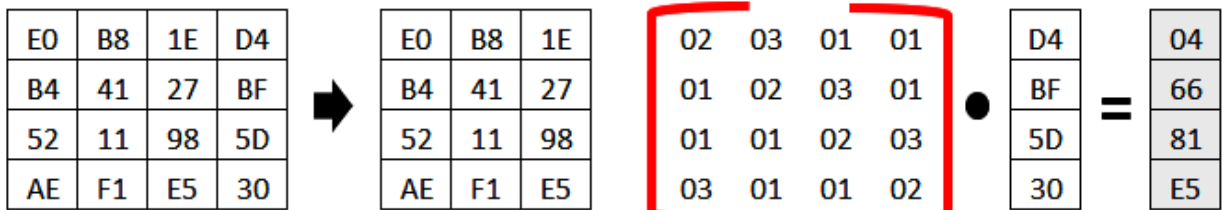
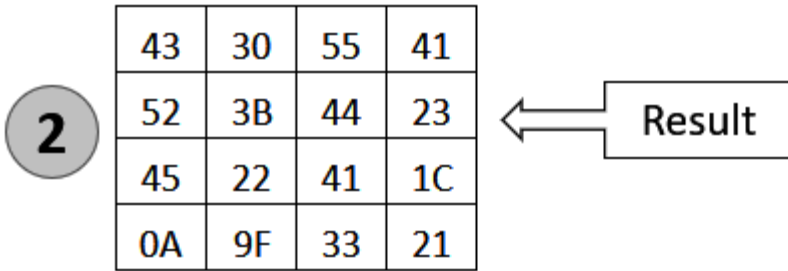
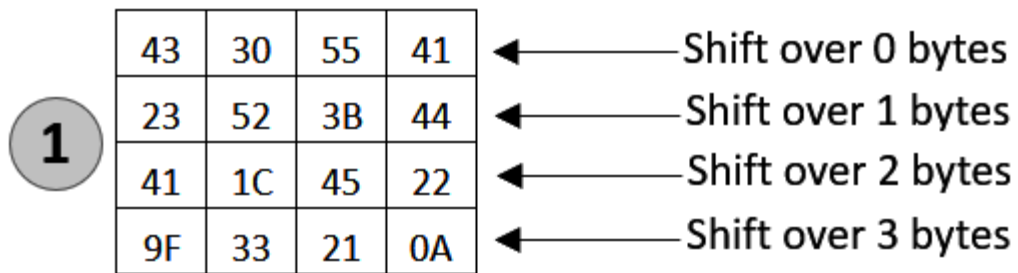


43	30	55	41
23	52	3B	44
41	1C	45	22
9F	33	21	0A

State Table

hex	y															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	79	9A	7B	6B	9C	A4	D3	BA	72	41	7B	D0	18	94	E7	22
1	B0	7F	D7	5A	41	8B	AE	6E	5B	9E	60	82	8C	AC	33	6D
2	D5	A3	3B	B1	44	A7	4F	48	8C	FC	9B	E6	DC	6F	BE	68
3	93	79	0C	9F	22	1F	22	9C	34	CF	B6	94	A4	5D	E7	BC
4	4F	DD	AC	09	0A	98	AC	7E	D5	62	B8	13	95	AD	C4	0A
5	16	E7	68	CA	40	C7	B6	9A	6E	A2	0F	9C	7C	E8	22	EA
6	C9	A3	D2	60	7B	AC	01	7B	2E	F1	5B	CA	64	DD	42	A7
7	0A	3B	21	E1	2C	28	3E	DA	A0	2F	9C	0A	79	18	ED	77
8	68	17	8F	AC	0A	E9	F2	99	D2	8E	54	F3	31	D7	6D	8A
9	31	64	85	97	7B	CE	9B	C2	E7	A6	2A	7A	57	C3	E7	0A
A	B4	7C	13	74	FF	B0	51	F1	BB	86	A6	F4	79	0A	C9	B8
B	18	56	30	EF	BD	25	73	9F	64	47	D2	AA	CE	F3	1E	A0
C	59	91	F9	51	F1	32	7E	EE	AC	39	4F	D5	EC	94	8F	98
D	79	6D	5E	2C	0A	18	2A	3E	5C	82	A3	FA	18	8D	57	A6
E	51	47	36	3C	0A	F4	23	07	D0	7A	39	A4	2D	99	62	E0
F	0A	38	12	B9	0A	BA	47	D1	20	A7	C6	4C	1D	50	0C	E9

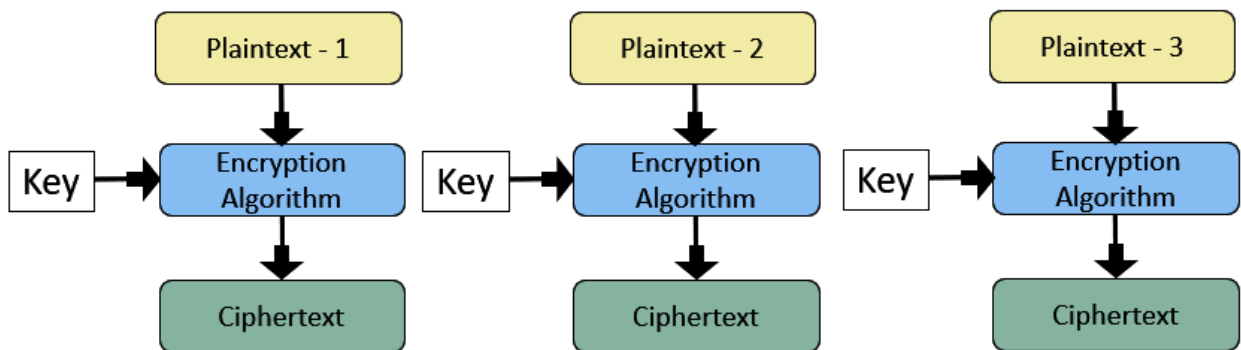
S-BOX

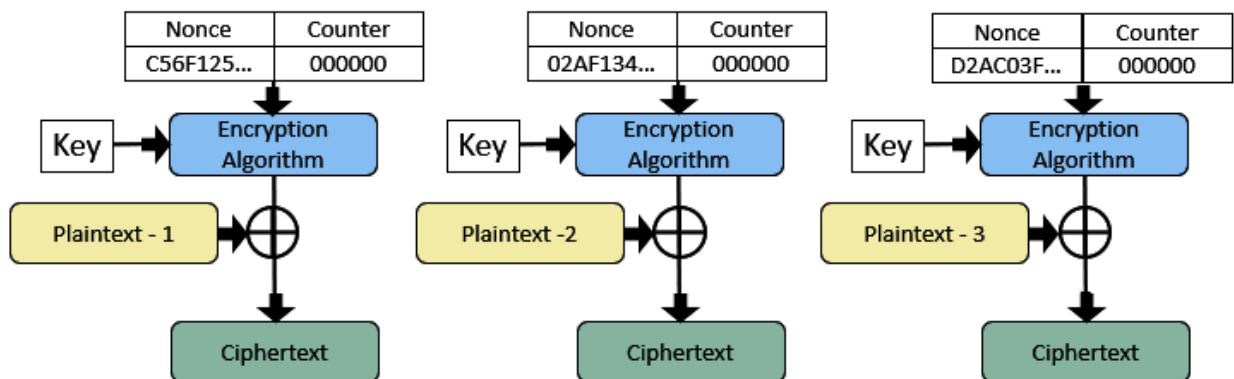
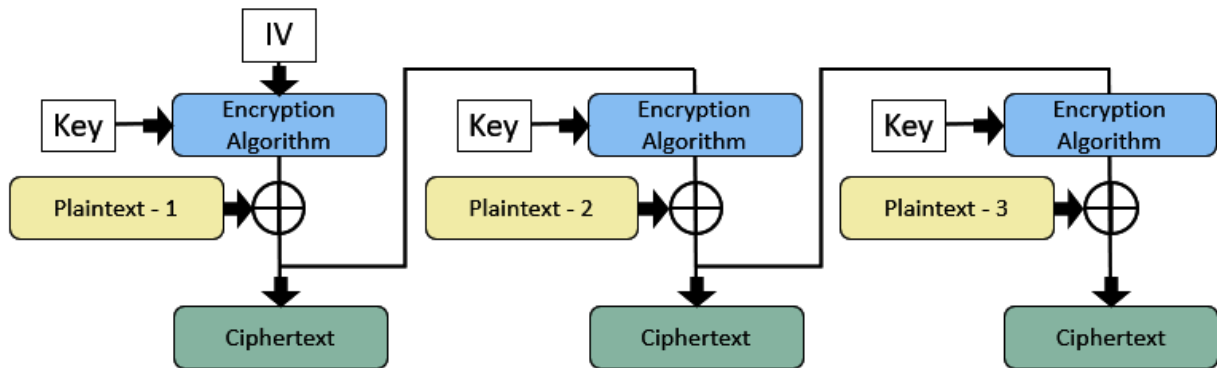
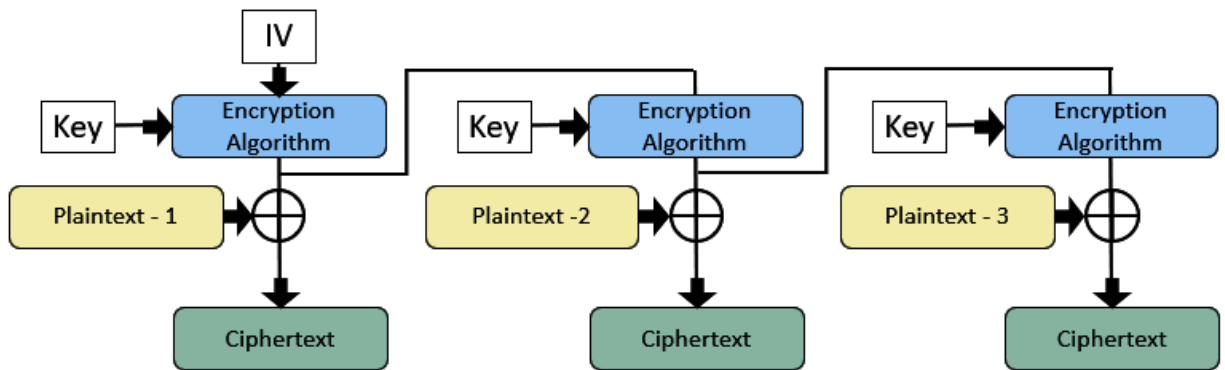
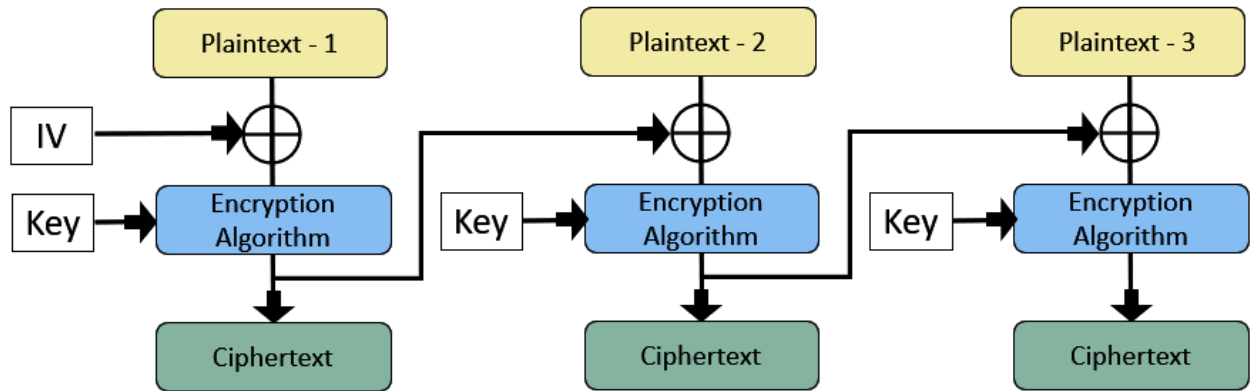


State Table

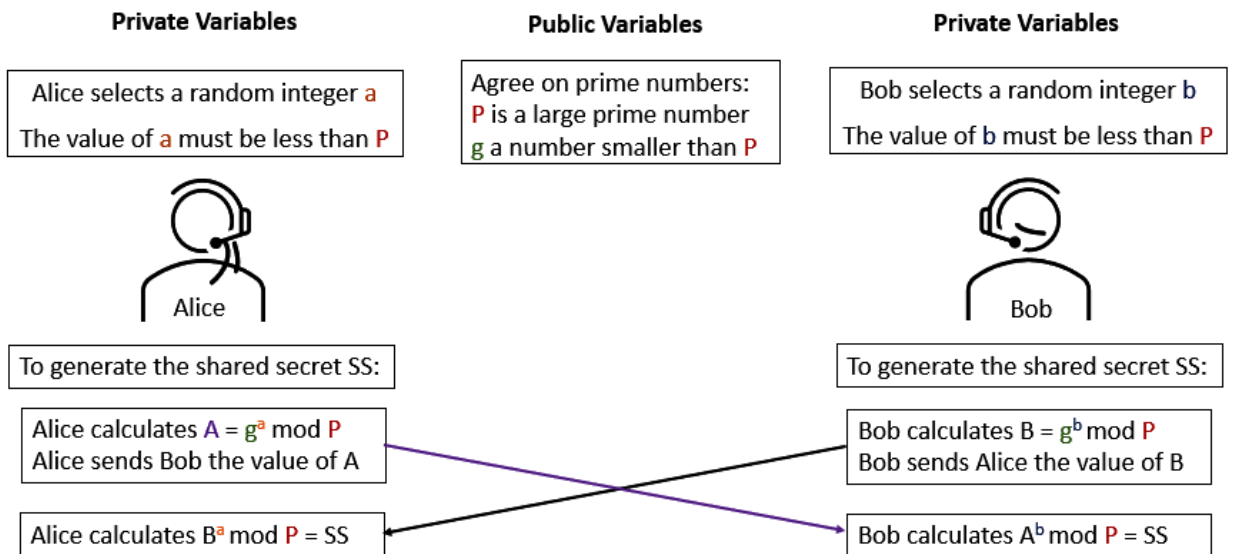
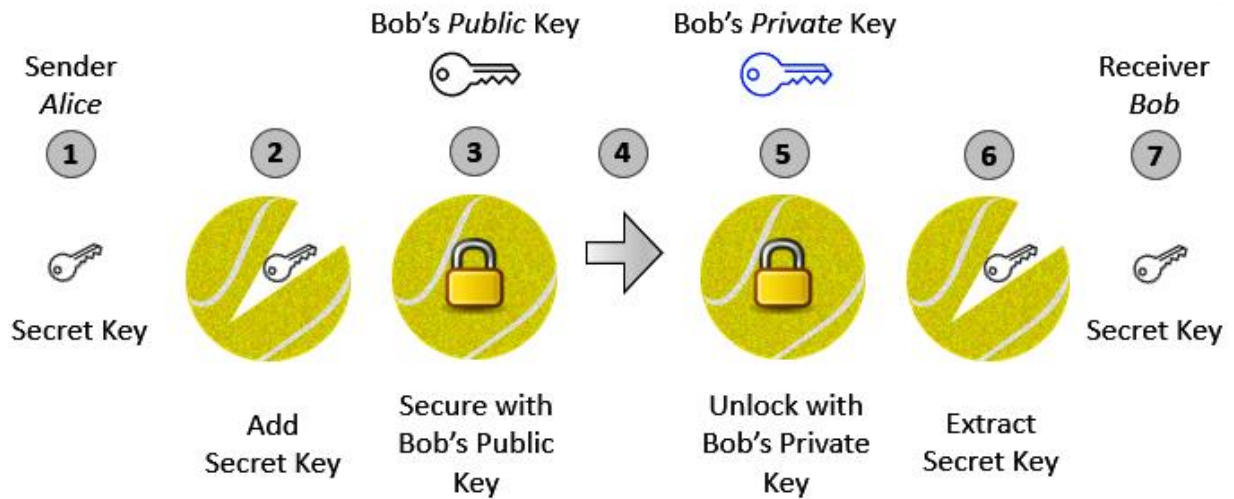
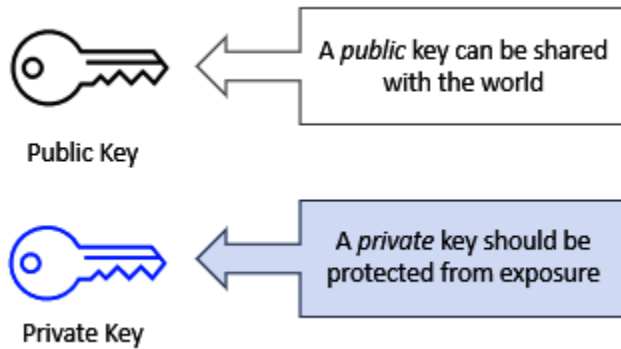
Matrix

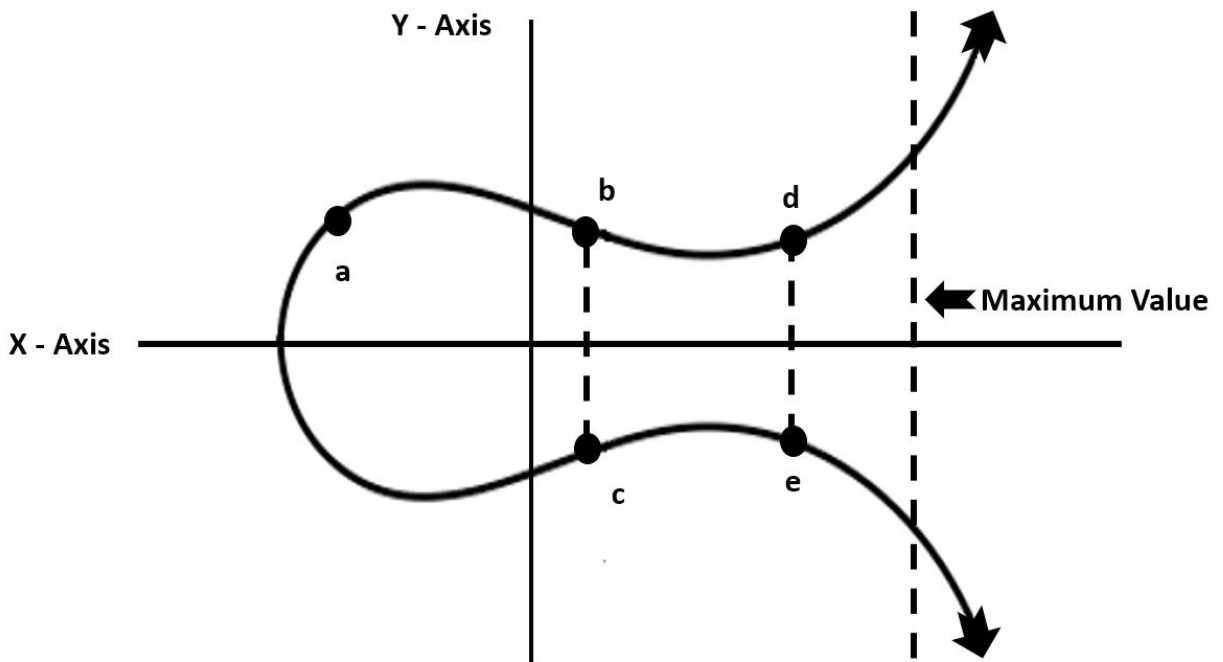
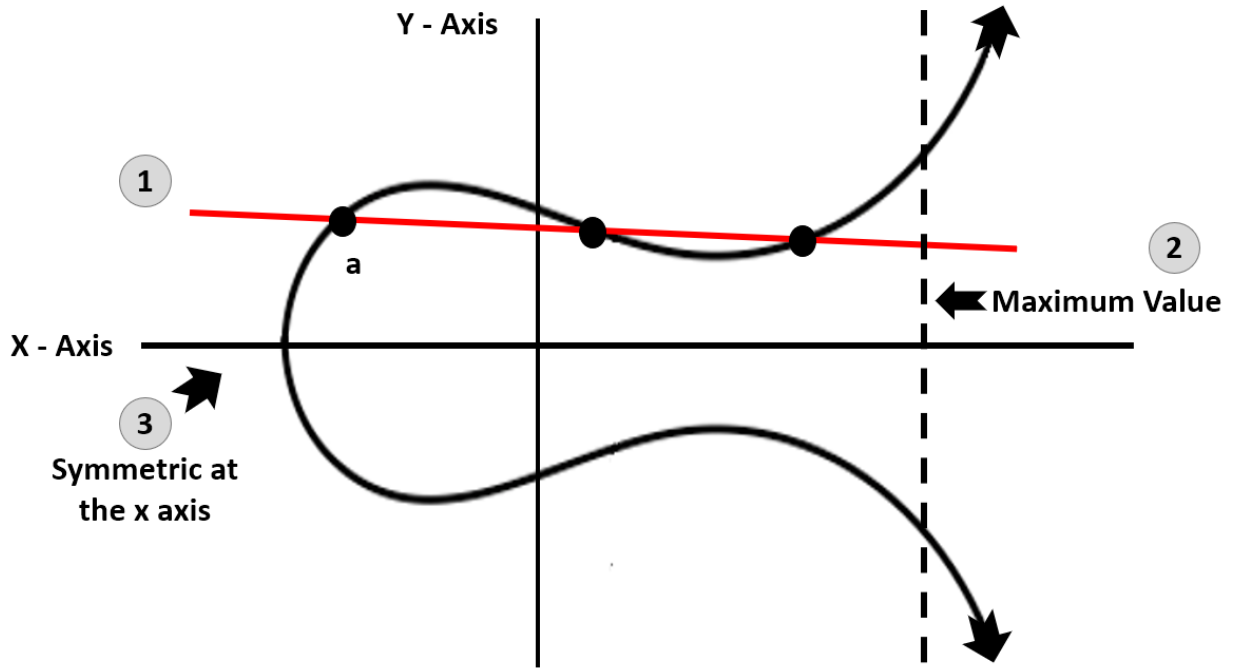
010110101110101001010100101010010101001

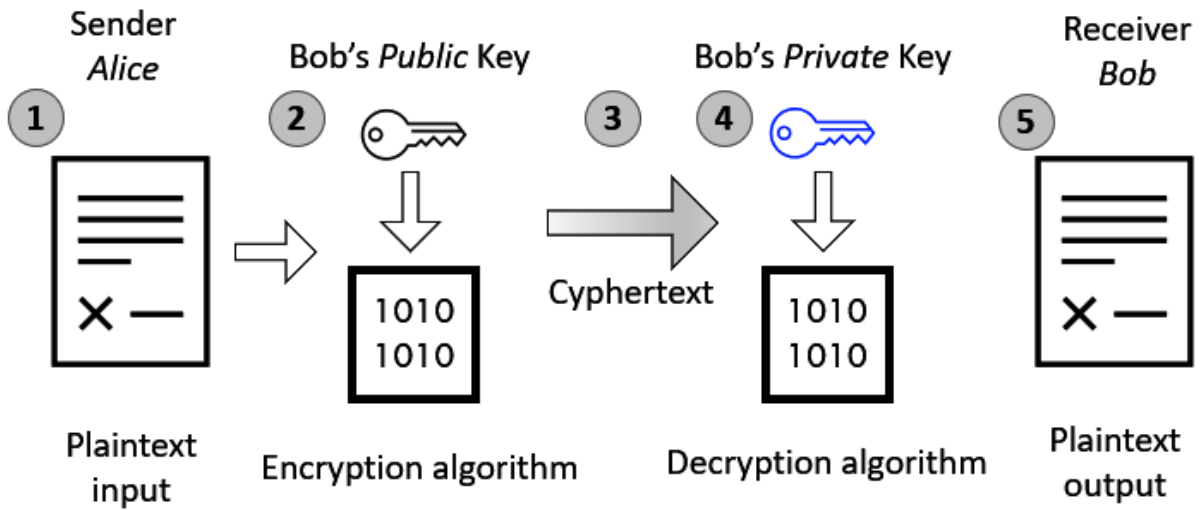
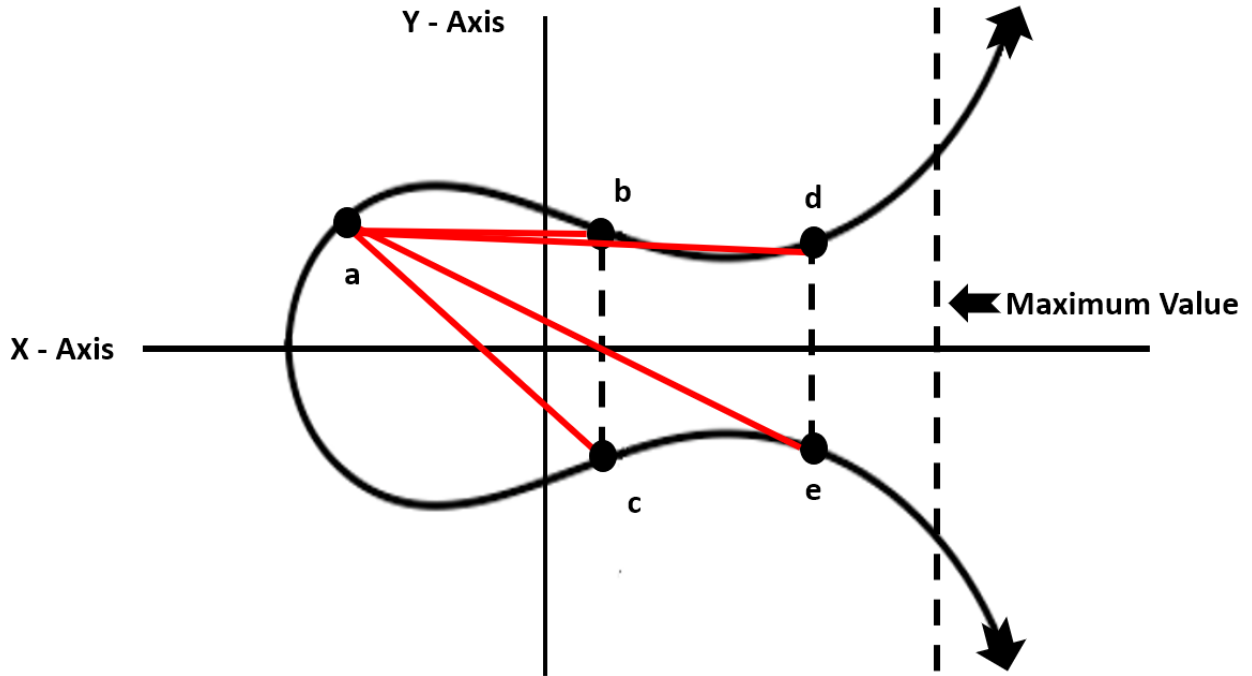


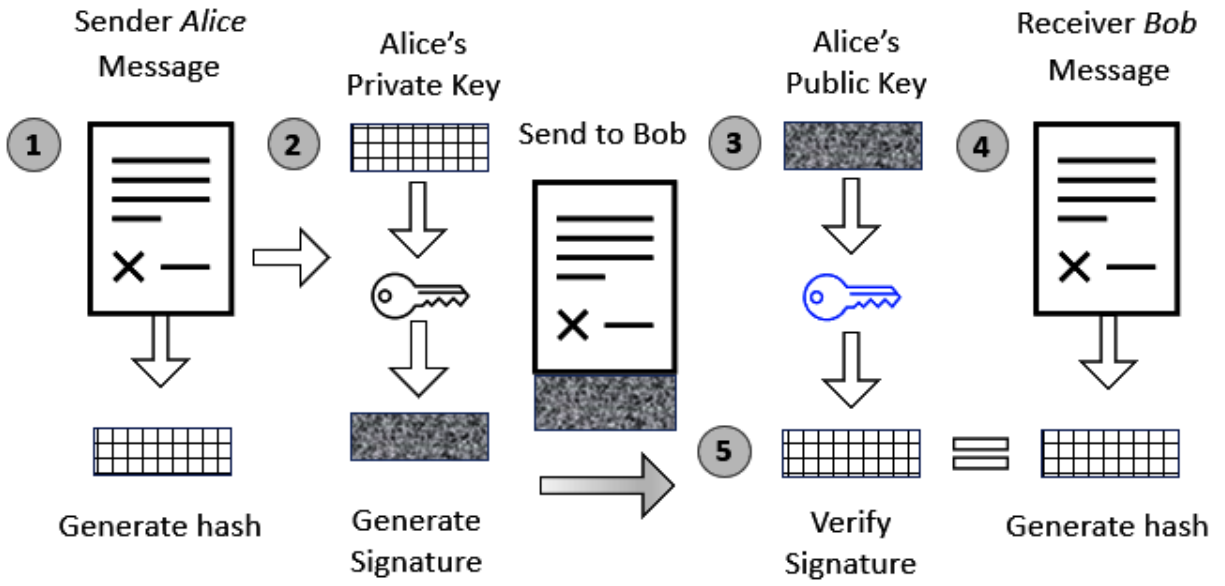


Chapter 5: Dissecting Asymmetric Encryption

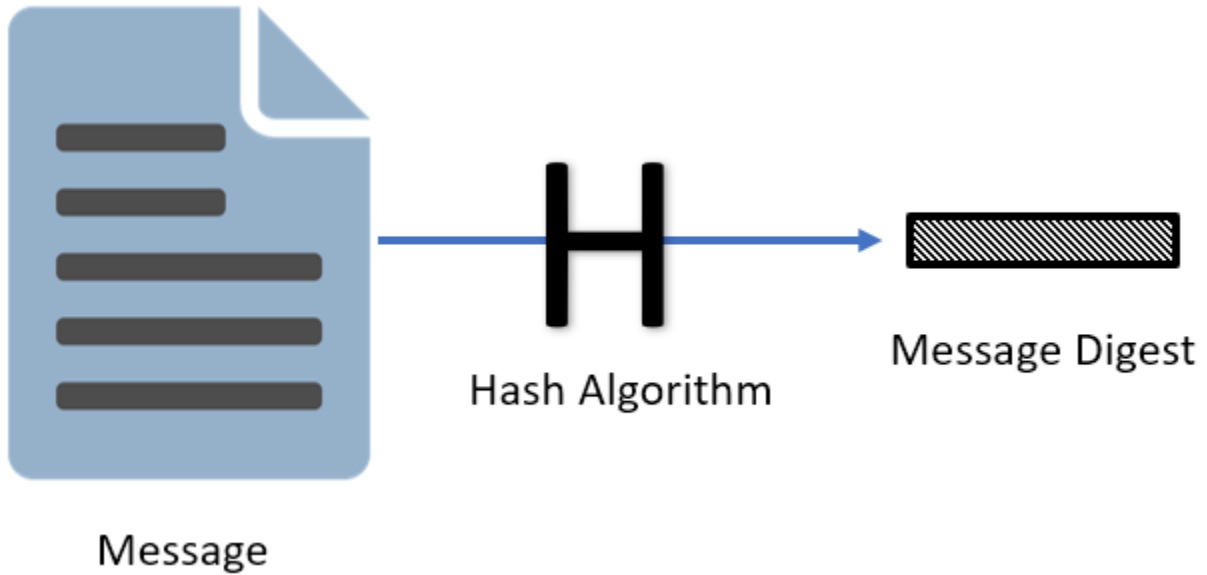






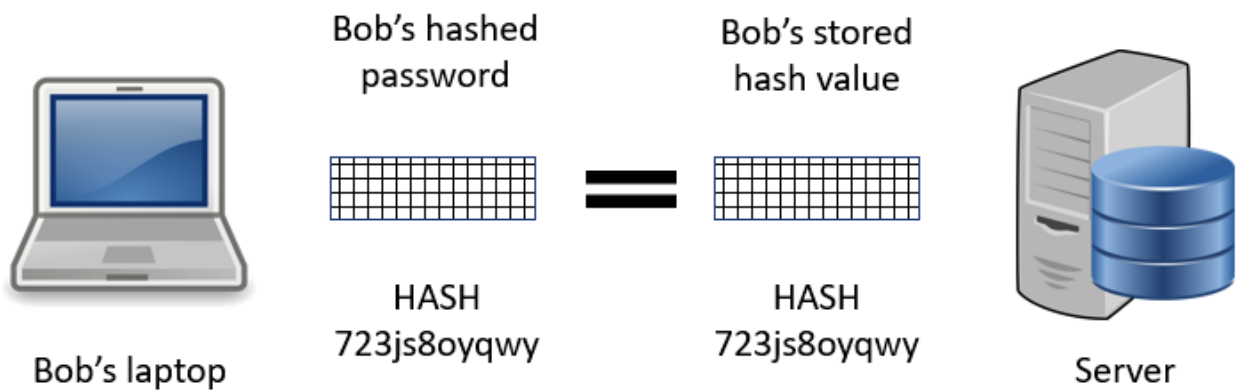
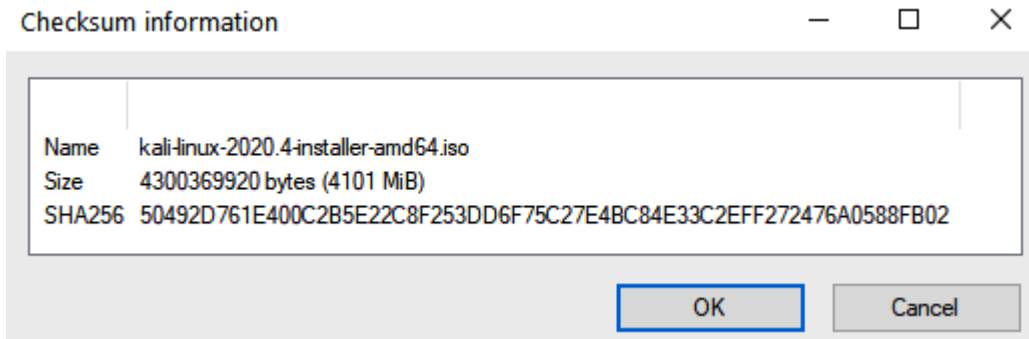
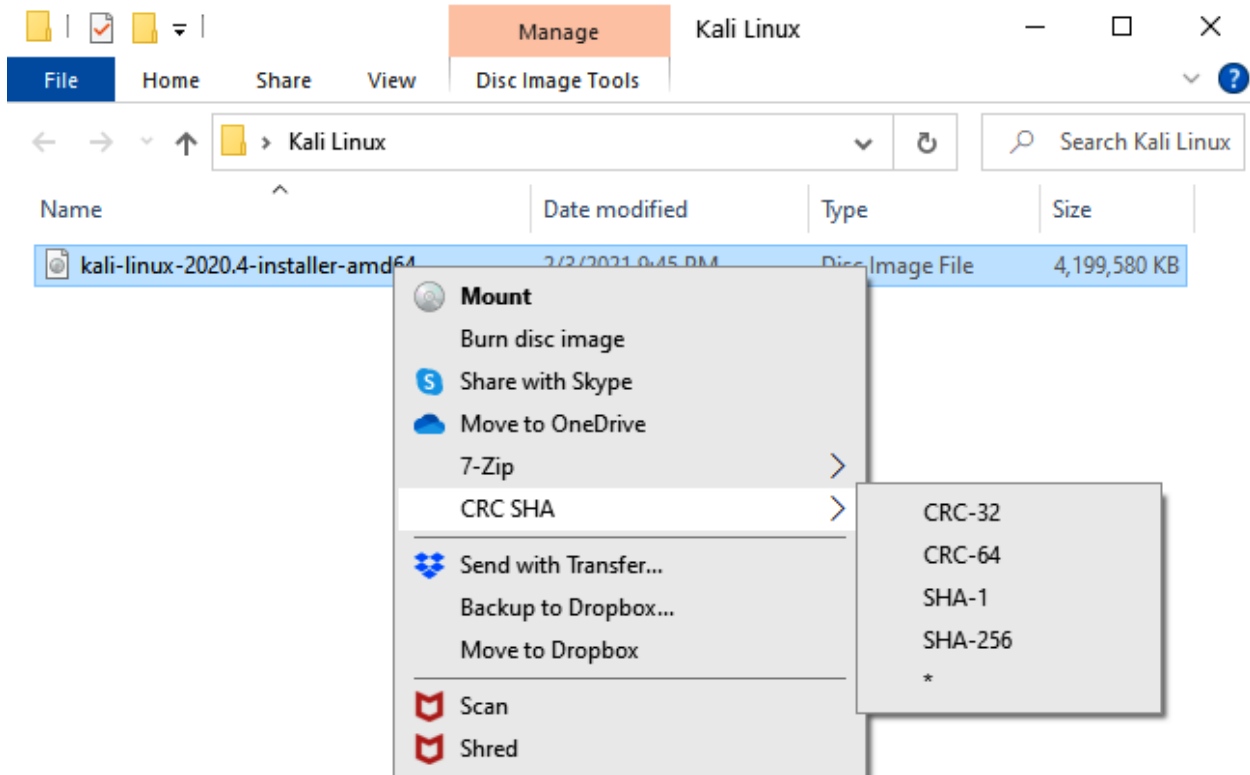


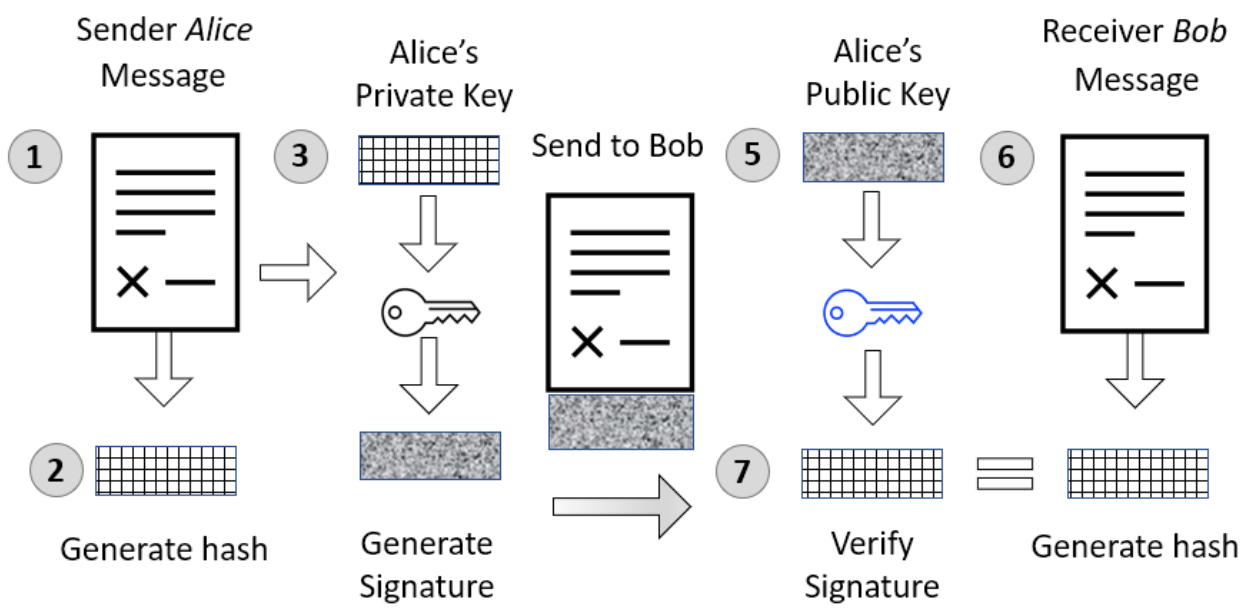
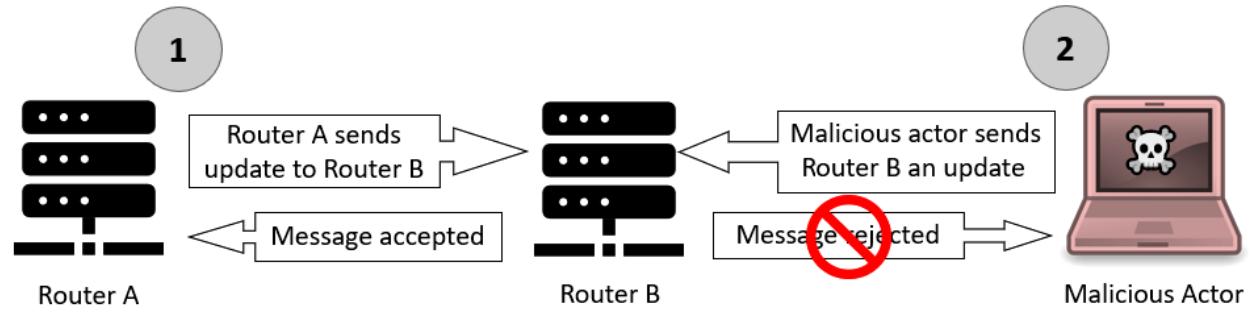
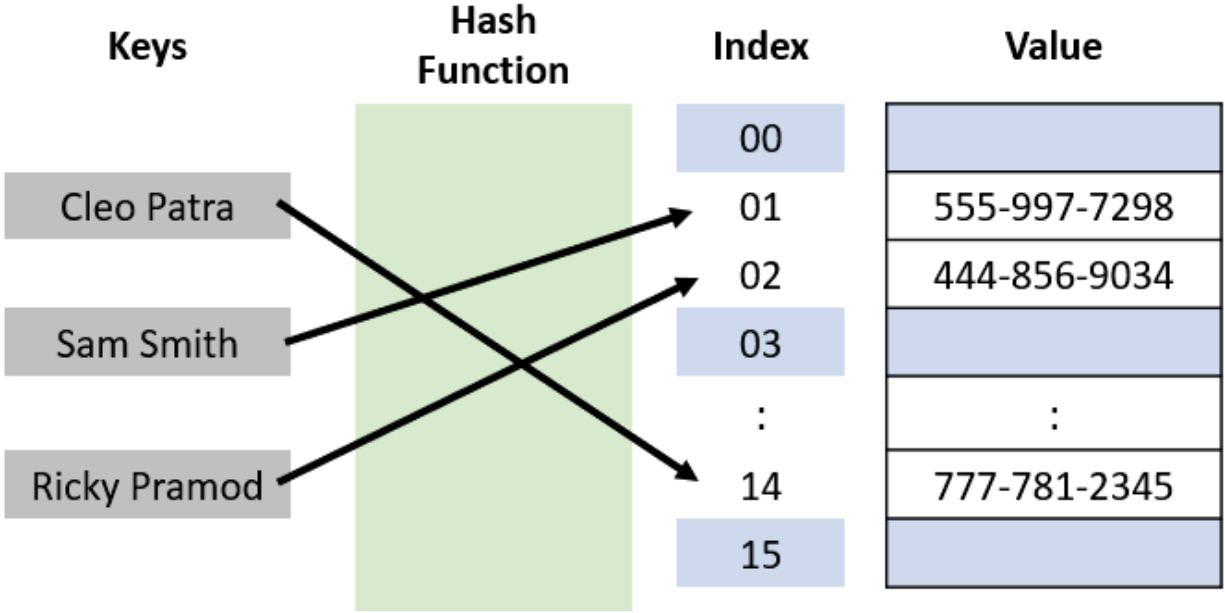
Chapter 6: Examining Hash Algorithms

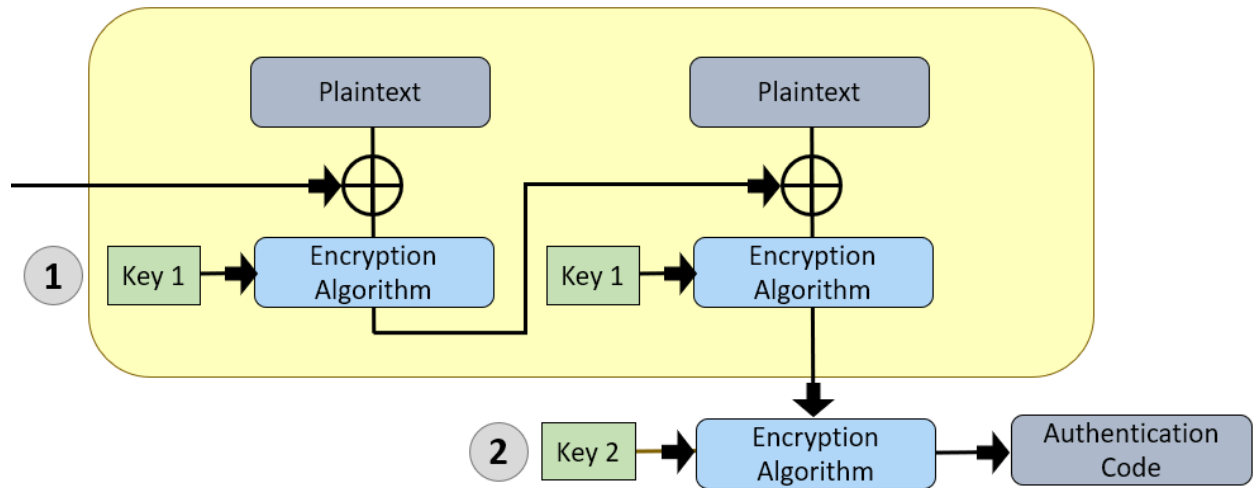
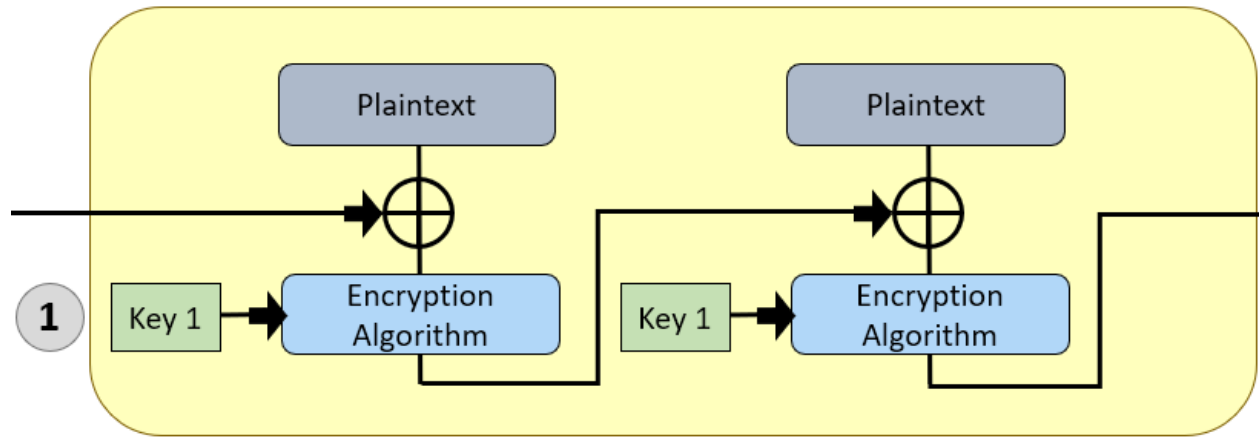


Hash Algorithm	Message Digest Output in Bits
SHA-2 (256)	256
SHA-2 (384)	384
SHA-2 (512)	512
Whirlpool	512

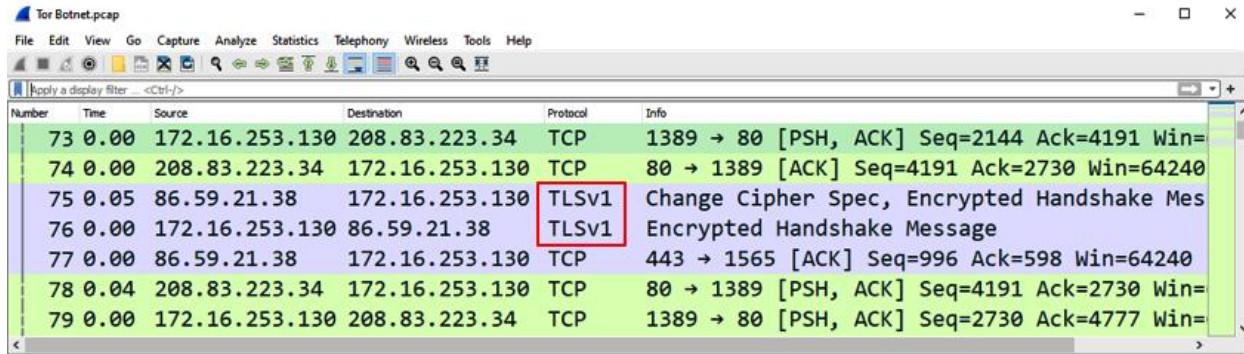
Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.4	41.G	50492d761e400c2b5e22c8f253dd6f75c27e4bc84e33c2eff272476a0588fb02







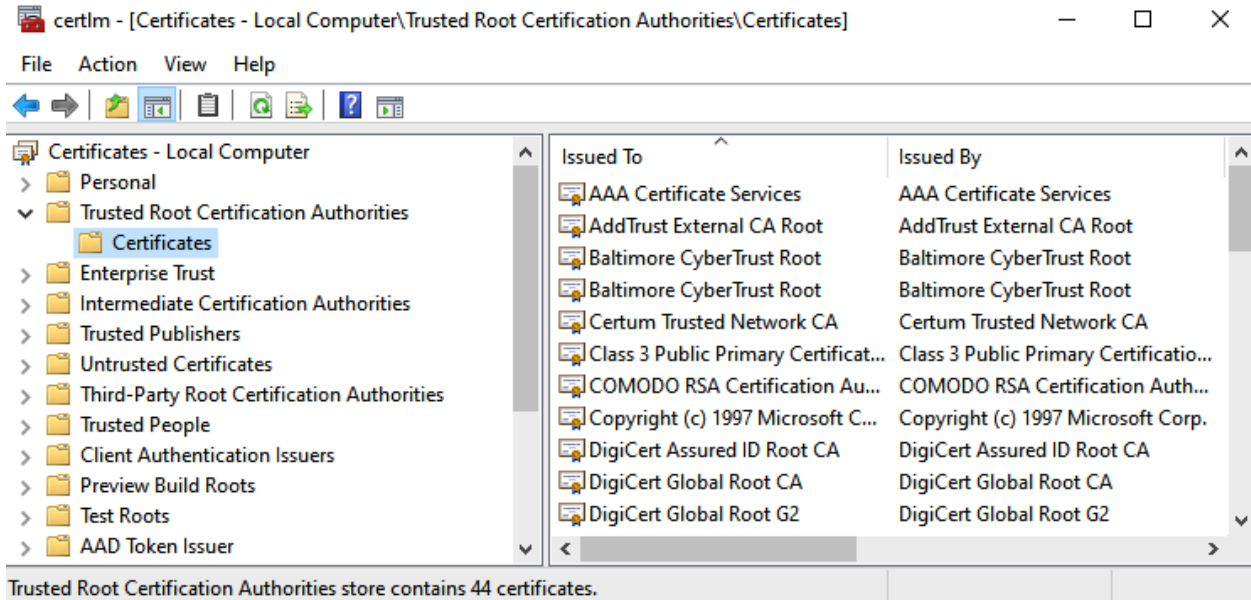
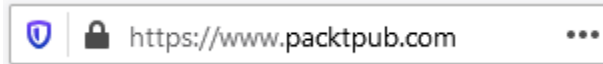
Chapter 7: Adhering to Standards



The screenshot shows a Wireshark interface with a network traffic capture. The main pane displays a list of packets with columns for Number, Time, Source, Destination, Protocol, and Info. Two packets, 75 and 76, are highlighted in blue and have their Protocol column value 'TLSv1' enclosed in a red box. Packet 75 is a 'Change Cipher Spec, Encrypted Handshake Message' and packet 76 is an 'Encrypted Handshake Message'. Other packets shown include TCP connections and acknowledgments between IP addresses 172.16.253.130 and 208.83.223.34.

Number	Time	Source	Destination	Protocol	Info
73	0.00	172.16.253.130	208.83.223.34	TCP	1389 → 80 [PSH, ACK] Seq=2144 Ack=4191 Win=
74	0.00	208.83.223.34	172.16.253.130	TCP	80 → 1389 [ACK] Seq=4191 Ack=2730 Win=64240
75	0.05	86.59.21.38	172.16.253.130	TLSv1	Change Cipher Spec, Encrypted Handshake Mes
76	0.00	172.16.253.130	86.59.21.38	TLSv1	Encrypted Handshake Message
77	0.00	86.59.21.38	172.16.253.130	TCP	443 → 1565 [ACK] Seq=996 Ack=598 Win=64240
78	0.04	208.83.223.34	172.16.253.130	TCP	80 → 1389 [PSH, ACK] Seq=4191 Ack=2730 Win=
79	0.00	172.16.253.130	208.83.223.34	TCP	1389 → 80 [PSH, ACK] Seq=2730 Ack=4777 Win=

Chapter 8: Using a Public Key Infrastructure



Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to www.google.com. The website is either misconfigured or your computer clock is set to the wrong time.

What can you do about it?

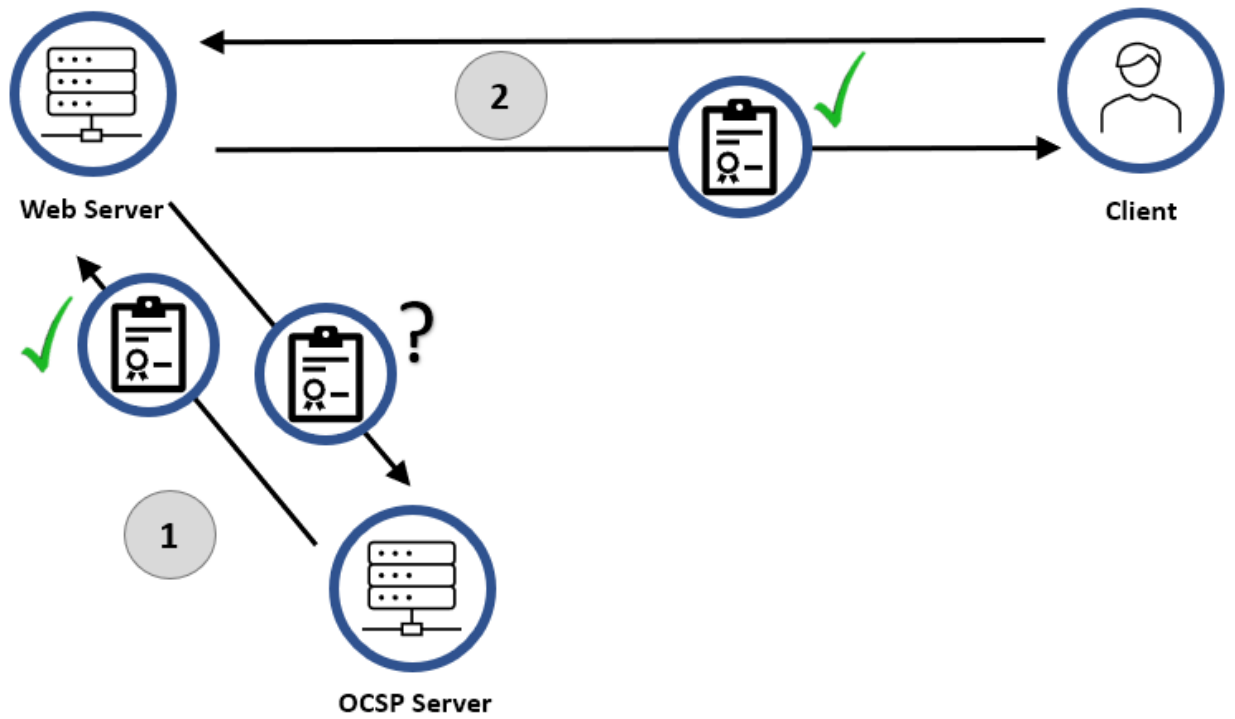
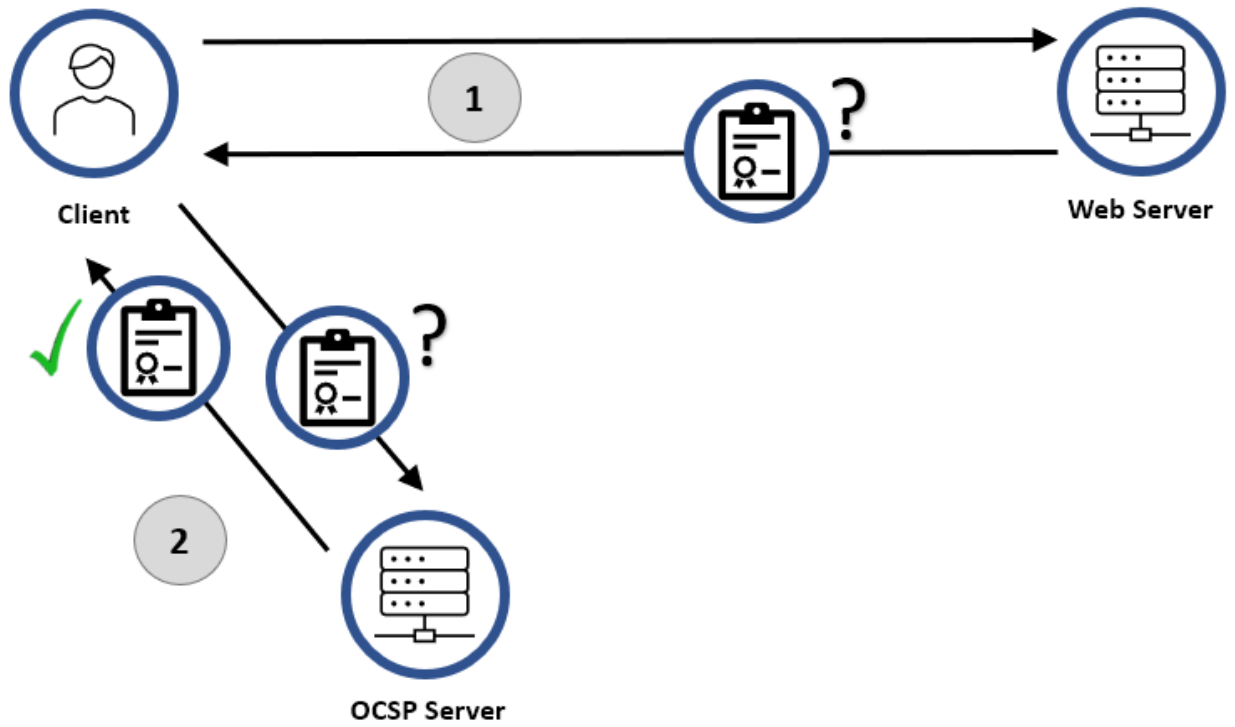
Your computer clock is set to 3/2/2039. Make sure your computer is set to the correct date, time, and time zone in your system settings, and then refresh www.google.com.

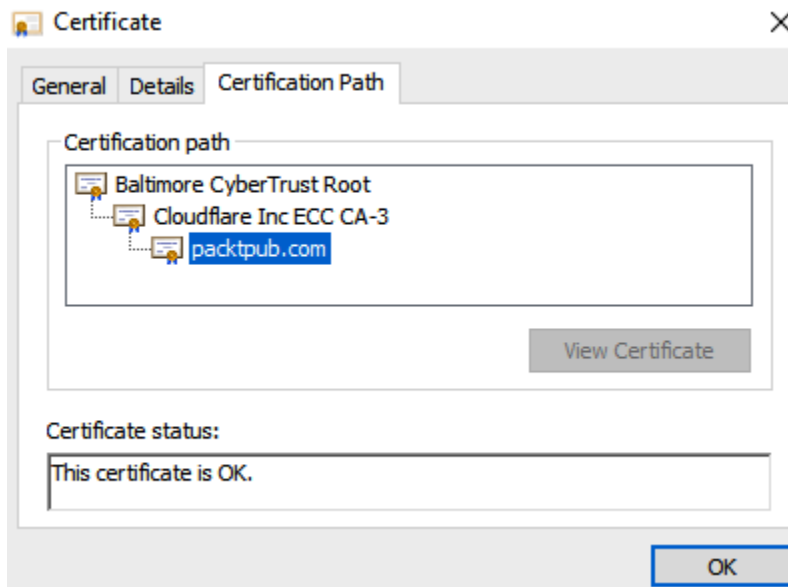
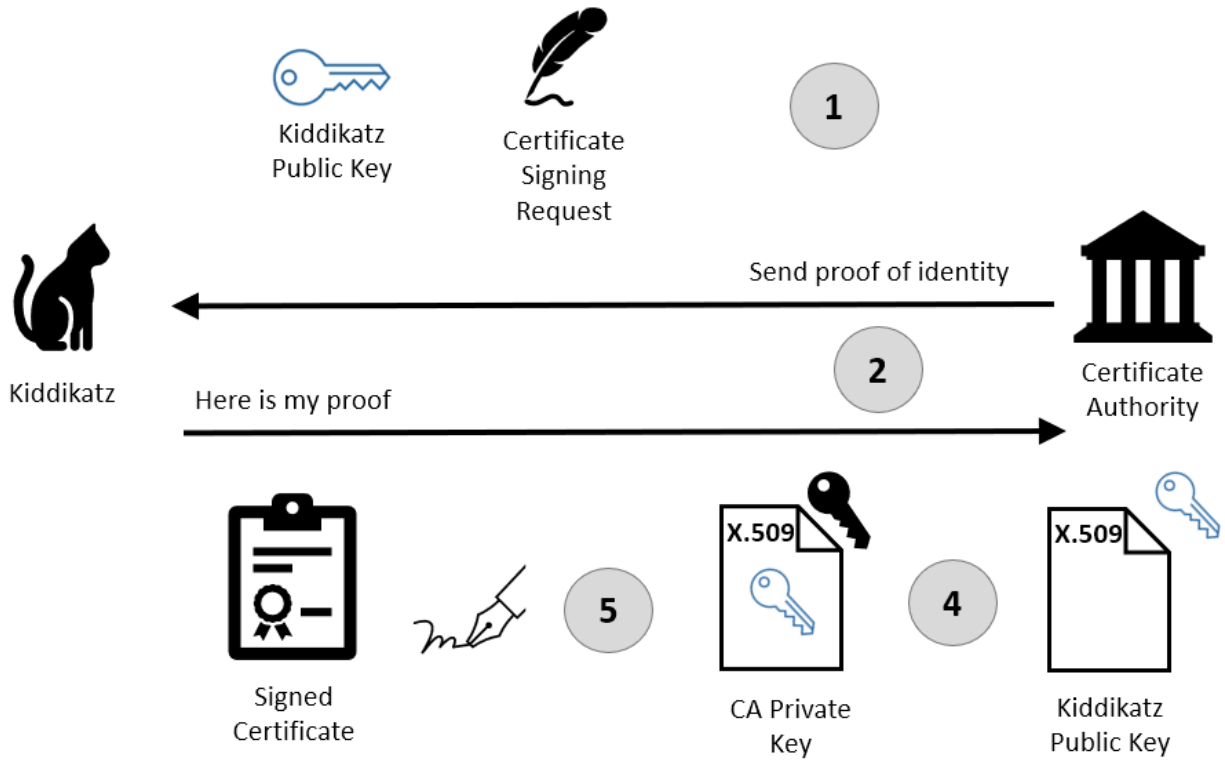
If your clock is already set to the right time, the website is likely misconfigured, and there is nothing you can do to resolve the issue. You can notify the website's administrator about the problem.

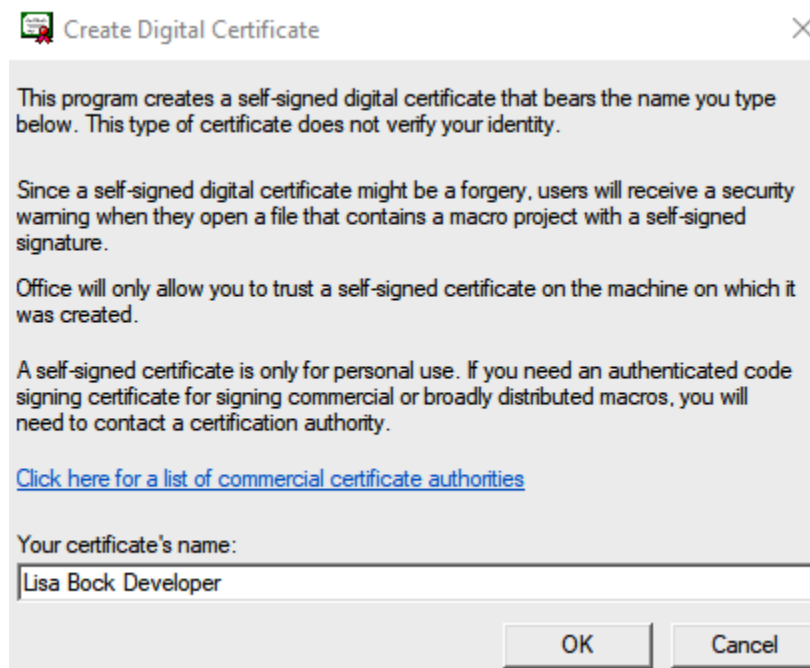
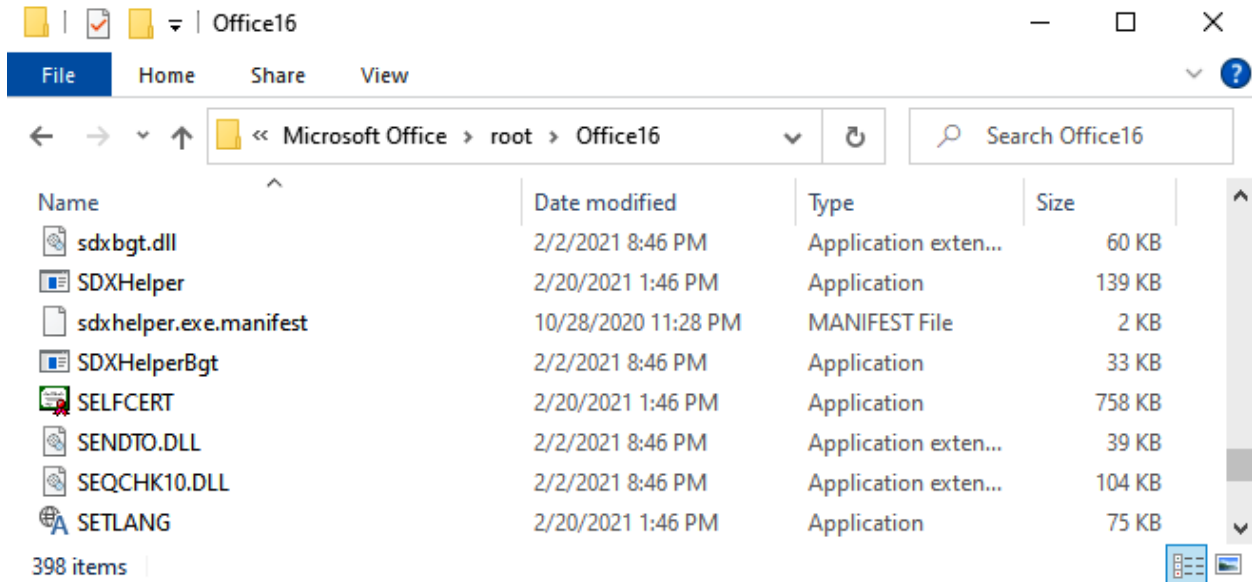
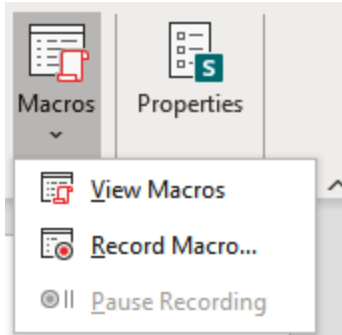
[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)







SelfCert Success



Successfully created a new certificate for Lisa Bock Developer.

OK

Internet Properties ? X

General Security Privacy **Content** Connections Programs Advanced

Certificates

Use certificates for encrypted connections and identification.

Clear SSL state Certificates Publishers

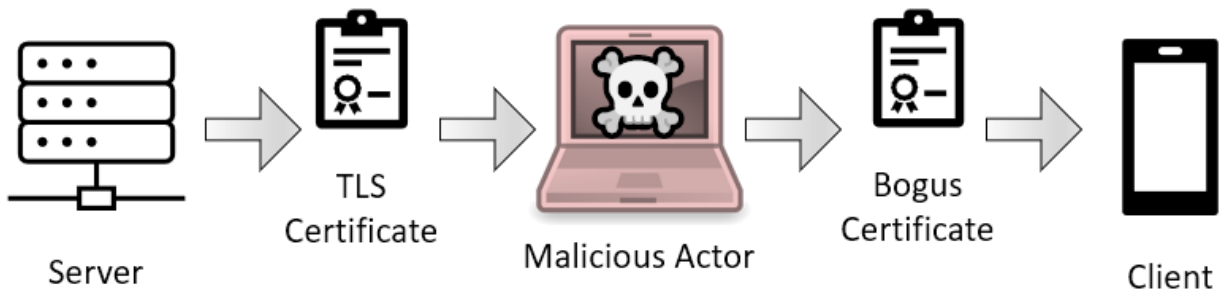
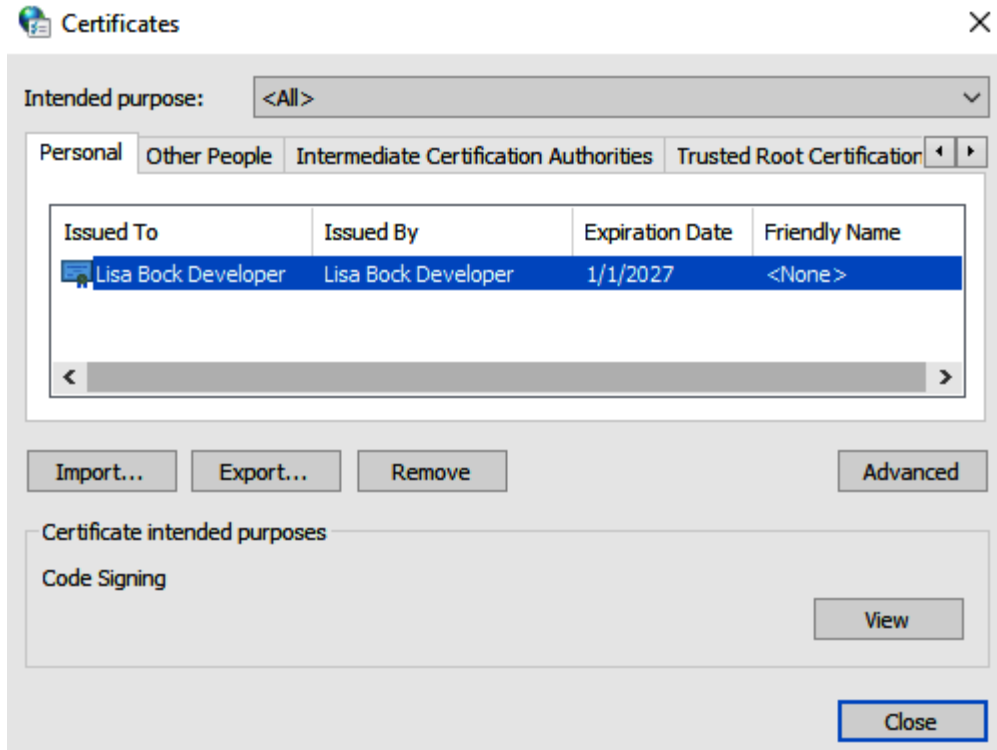
AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you. Settings

Feeds and Web Slices

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs. Settings

OK Cancel Apply





General



Media



Permissions



Security

Website Identity

Website: www.google.com

Owner: This website does not supply ownership information.

Verified by: Google Trust Services

[View Certificate](#)

Expires on: Tuesday, April 20, 2021

Privacy & History

Have I visited this website prior to today? Yes, 1,235 times

Is this website storing information on my computer? Yes, cookies and 10.8 MB of site data

[Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No

[View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

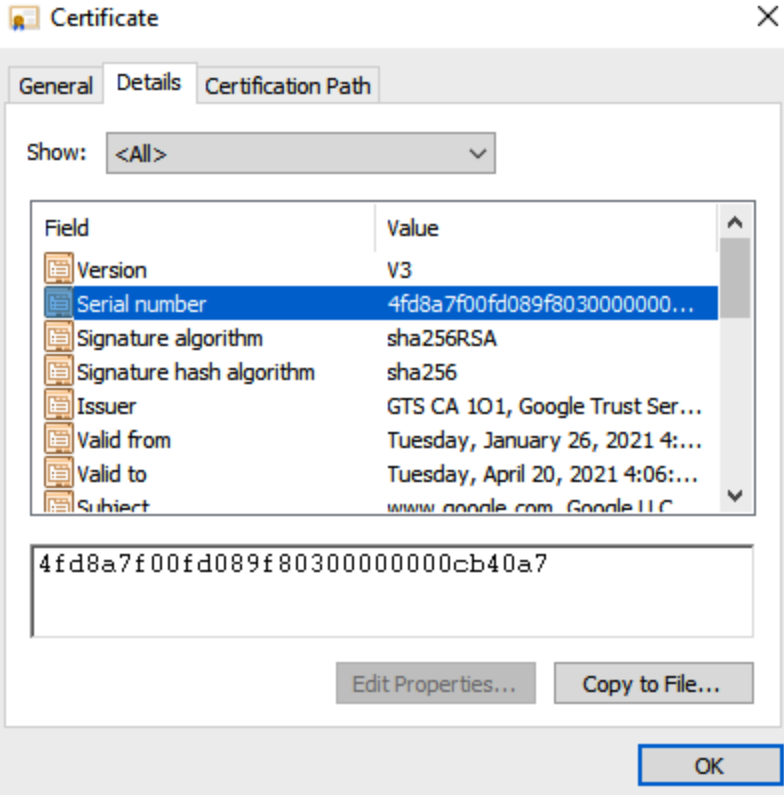
File Edit View History Bookmarks Tools Help

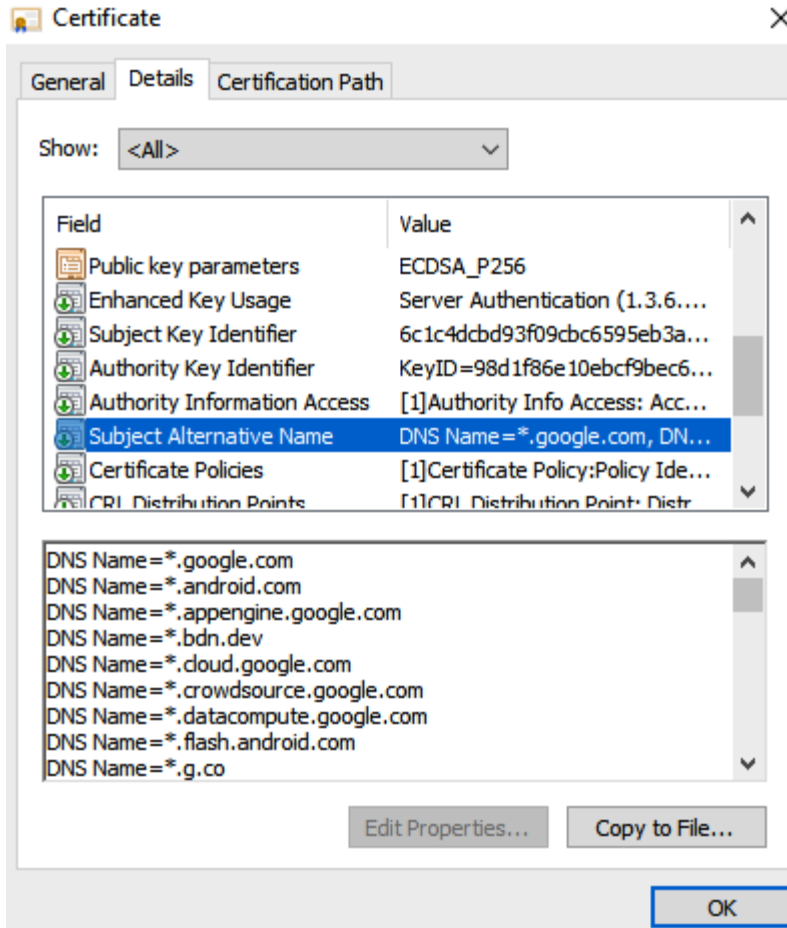
Google Certificate for www.google.com

Firefox about:certificate?cert=MIIExzCCA6%2Bg


Certificate

www.google.com	GTS CA 101	GlobalSign
Subject Name		
Country	US	
State/Province	California	
Locality	Mountain View	
Organization	Google LLC	
Common Name	www.google.com	
Issuer Name		
Country	US	
Organization	Google Trust Services	
Common Name	GTS CA 101	





Chapter 9: Exploring IPsec and TLS




Version: 2021.1.27
Rulesets version for EFF (Full): 2021.3.4

HTTPS Everywhere is ON

Encrypt All Sites Eligible is OFF
Unencrypted requests are currently allowed

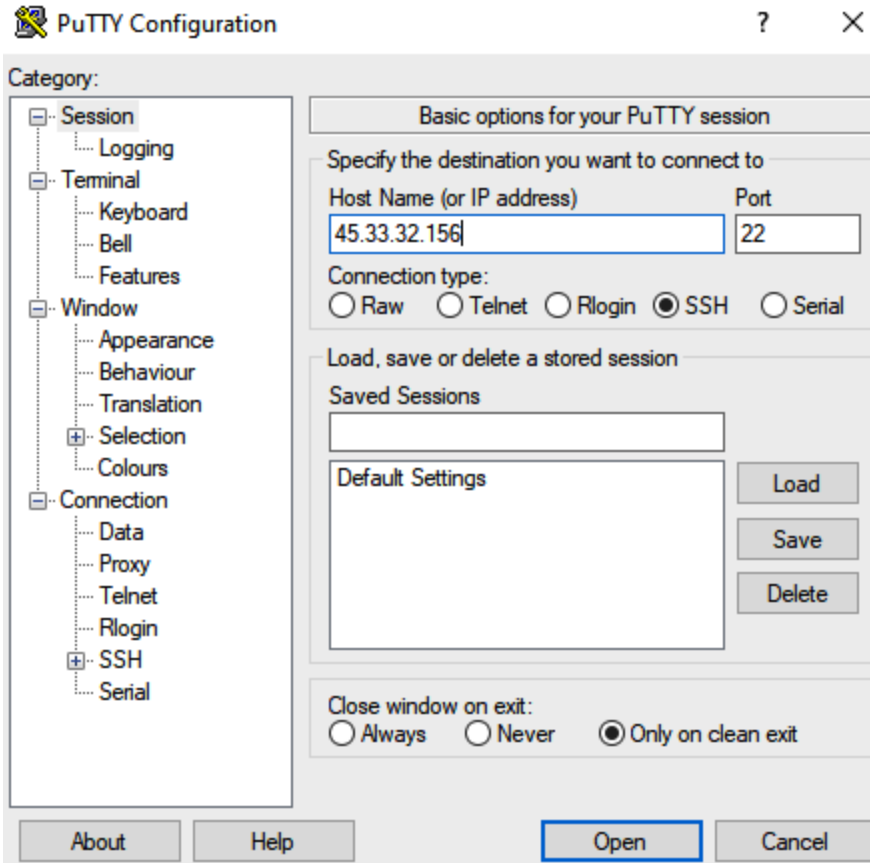
Settings for this site
Change your preferences for encrypted connections

[Disable on this site](#)

[See more](#) 

[Reset to Defaults](#)

[View All Rules](#) [About HTTPS Everywhere](#) [Donate to EFF](#)



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa  
AAAAB3NzaC1yc2EAAAABJQAAAQEAj7+R8xEI99LOEwrJwGMCWXcemCZSReNLe0  
y4UllgCjPRsBz/YZ32Pzvj2I27+XREldRTuN8g81li6cyQ6wAPYxxgj43rD9uEhSn9NOrY  
A8Di/LUNmKFz4yBPEj3NvVXX652sPFvyZKu  
+O0Dlo1u4WXk0B7drPxeUHJB/828VMHmSH/43A2YPnovzZFAEWNDHzG1/NoZX
```

Key fingerprint: ssh-rsa 2048 d0:a8:06:91:d1:cf:a2:fc:21:a1:f1:05:7:14:14:f3

Key comment: Edge_Router

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:
 RSA DSA ECDSA Ed25519 SSH-1 (RSA)

Number of bits in a generated key:

Settings

Home

Find a setting

Network & Internet

- Status
- Wi-Fi
- Ethernet
- Dial-up
- VPN**
- Airplane mode
- Mobile hotspot
- Proxy



VPN

+ Add a VPN connection

Advanced Options

Allow VPN over metered networks

On

Allow VPN while roaming

On

Related settings

[Change adapter options](#)

[Change advanced sharing options](#)

[Network and Sharing Center](#)

[Windows Firewall](#)


Help from the web

[Setting up a VPN](#)



Add a VPN connection

VPN provider

Windows (built-in) 


Connection name

Server name or address

VPN type

Automatic 

Type of sign-in info

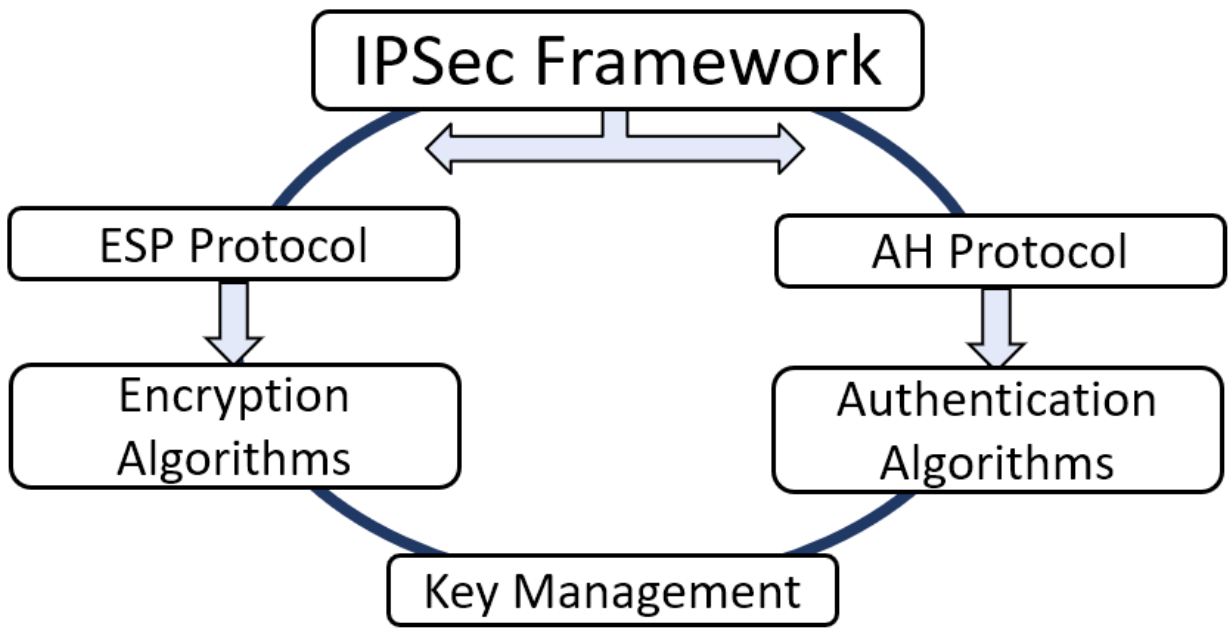
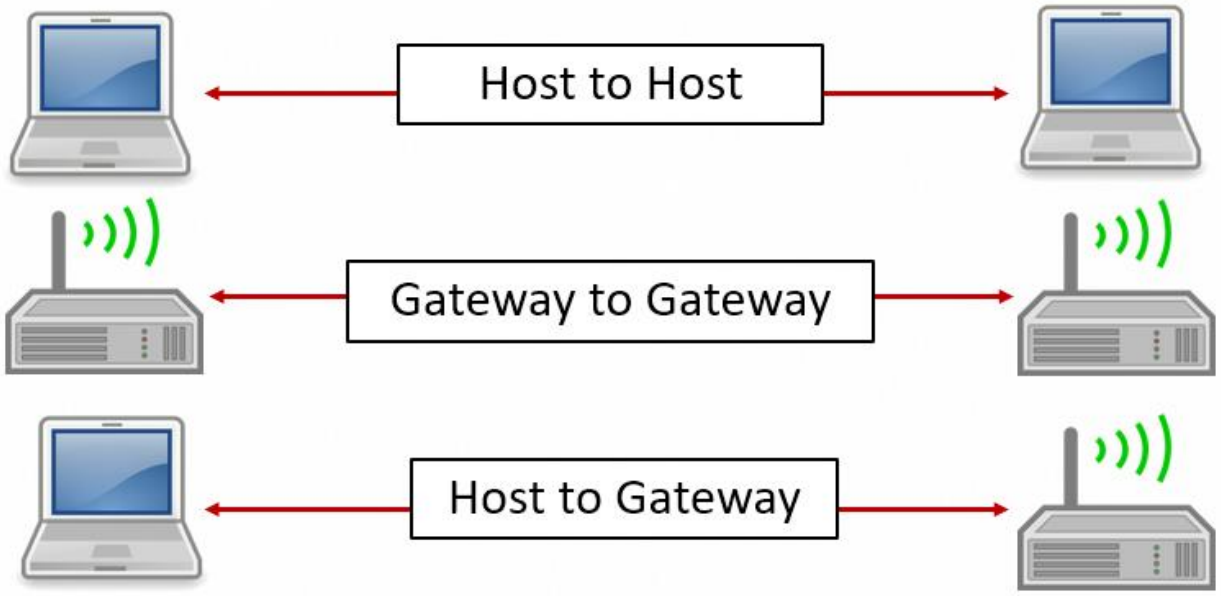
User name and password 

User name (optional)

Password (optional)

Save

Cancel





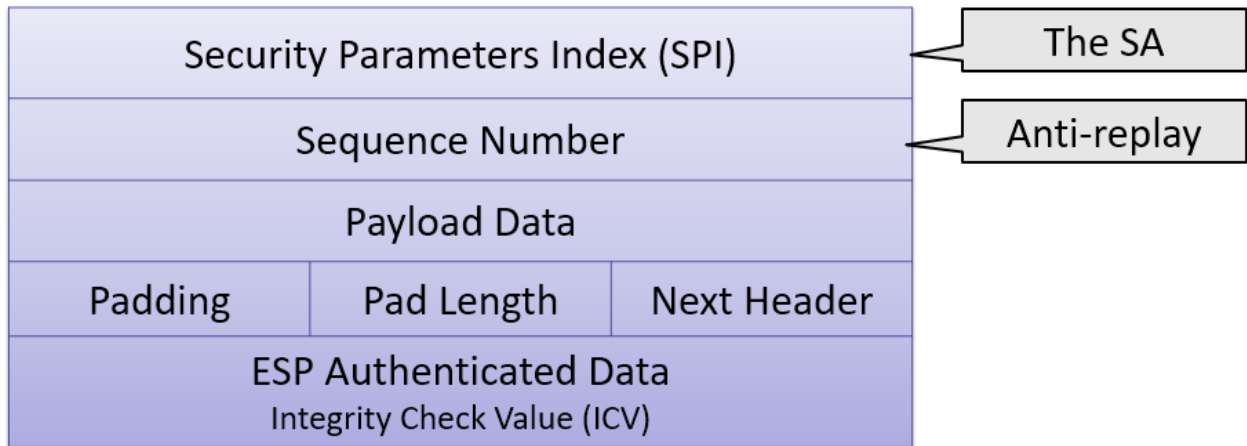
Router

1 inbound esp sas:
spi: 0xa6d5549285150c9c 2
3 transform: esp-aes,
in use settings={Tunnel, } 4
slot: 0. conn id: 17
cryptomap:PacktMap
sa timing: (k/sec)
replay detection support: N

▼ Encapsulating Security Payload
ESP SPI: 0x49507636 (1230009910)
ESP Sequence: 541414224

Next Header	Payload Length	<i>Reserved</i>	
Security Parameters Index (SPI)			The SA
Sequence Number			Anti-replay
AH Authenticated Data Integrity Check Value (ICV)			

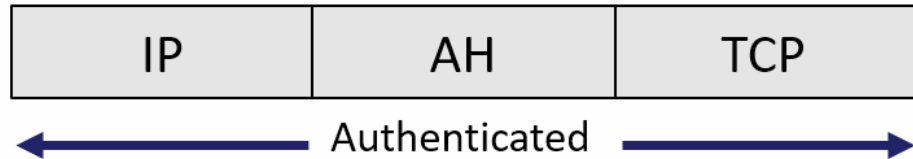
- > Frame 1: 194 bytes on wire (1552 bits), 194 bytes captured
- > Ethernet II, Src: c2:00:57:75:00:00 (c2:00:57:75:00:00), D
- > Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
- > Authentication Header
 - Next header: Encap Security Payload (50)
 - Length: 4 (24 bytes)
 - Reserved: 0000
 - AH SPI: 0x8179b705
 - AH Sequence: 1
 - AH ICV: 27cfc0a5e43d69b3728ec5b0
 - > Encapsulating Security Payload



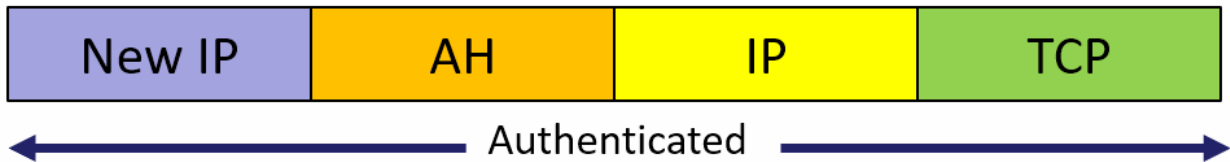
Original IP Packet



AH Transport Mode



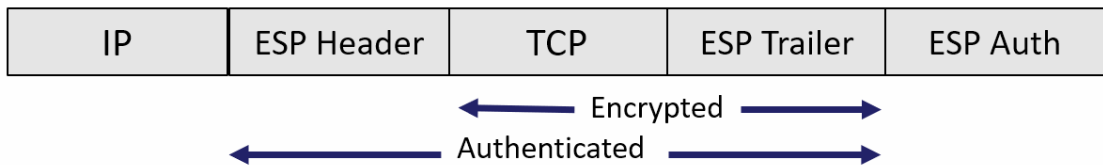
AH Tunnel Mode



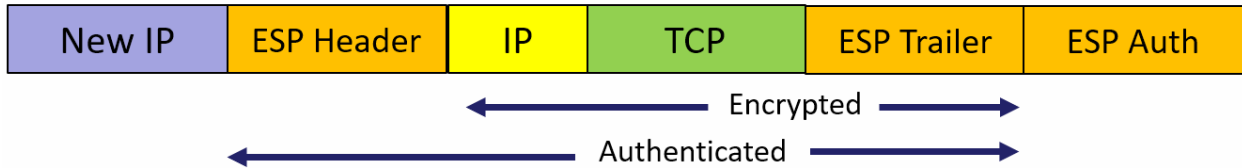
Original IP Packet



ESP Transport Mode



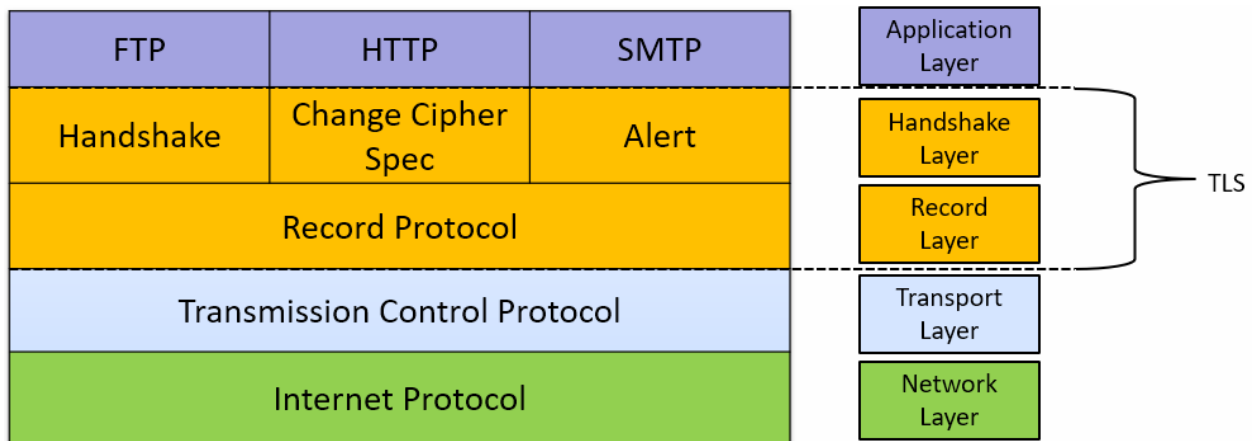
ESP Tunnel Mode

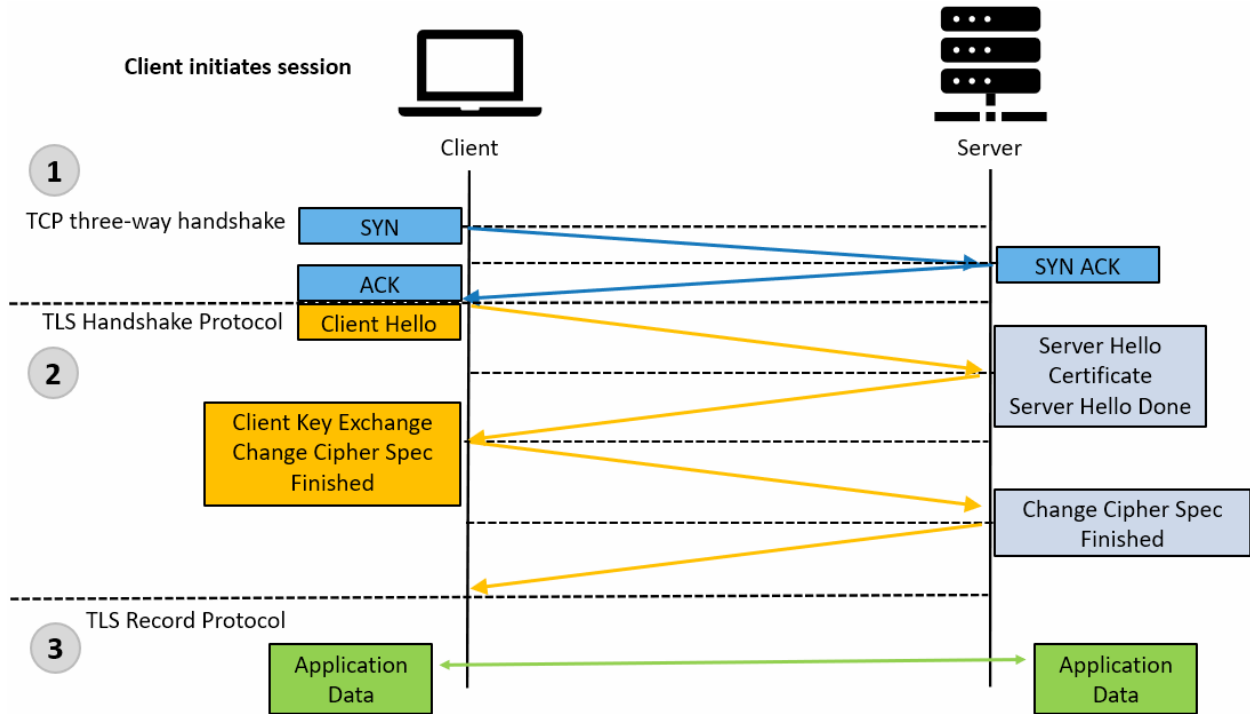


- DH Group 15 (3072-bit)
- DH Group 16 (4096-bit)
- DH Group 17 (6144-bit)

Add/Edit a New IPsec Profile

Keying mode:	Auto or manual
IKE Version:	IKEv1 or IKEv2
Phase 1 Options	
DH Group:	Group 17 - 6144-bit
Encryption:	AES-CBC 256
Authentication:	SHA2-256
SA Lifetime:	28800
Phase 2 Options	
Protocol Selection:	ESP or AH
Encryption:	AES-CBC 256
Authentication:	SHA2-256
SA Lifetime:	3600
Perfect Forward Secrecy:	Enable
DH Group:	Group 15 – 3072-bit





Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 229

Version: TLS 1.2 (0x0303)

Random: 2635fafc16c49a3e997ef714c303806dc8dbf634a2005b0e0186521c4ad6f9df

Session ID Length: 32

Session ID: 23c3a84ca631f3a948d15d929c972e00dded0857f2a00fbadd56175c4e362b84

Cipher Suites Length: 36

> Cipher Suites (18 suites)

Compression Methods Length: 1

> Compression Methods (1 method)

Extensions Length: 120

> Extension: renegotiation_info (len=1)

Cipher Suites (18 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

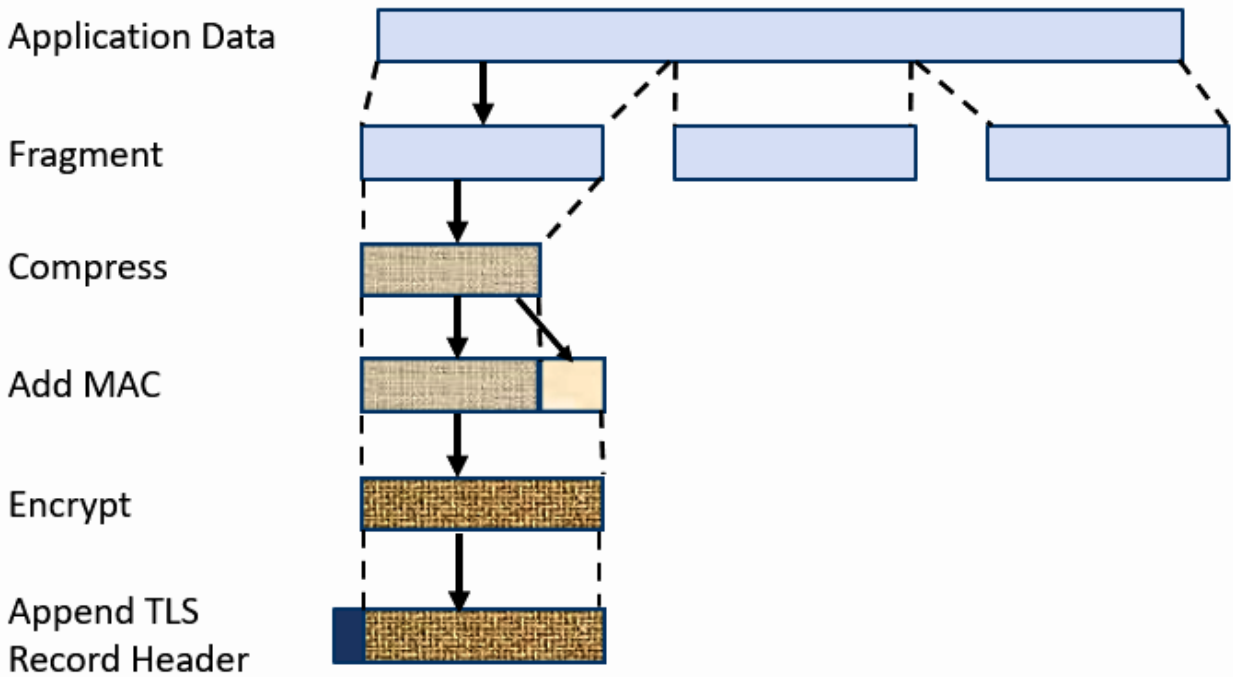
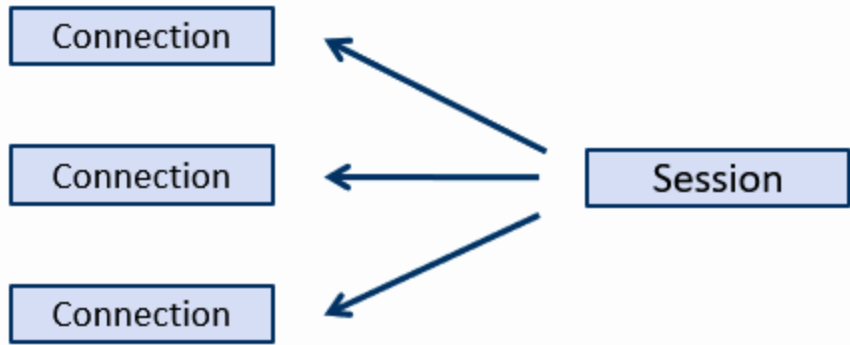
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

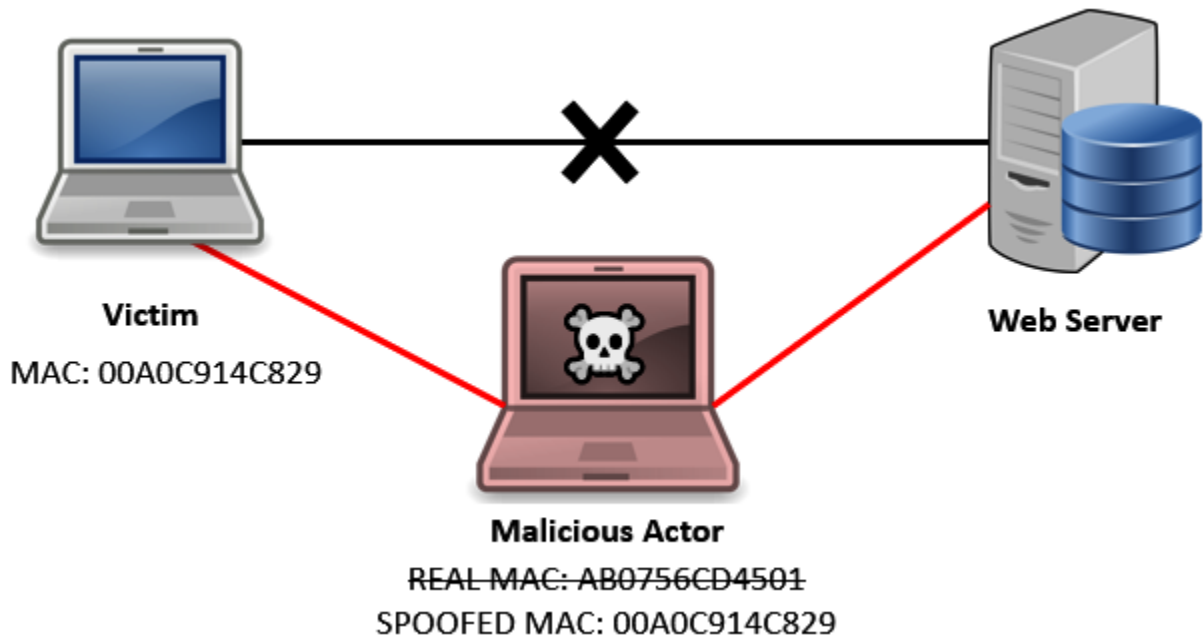
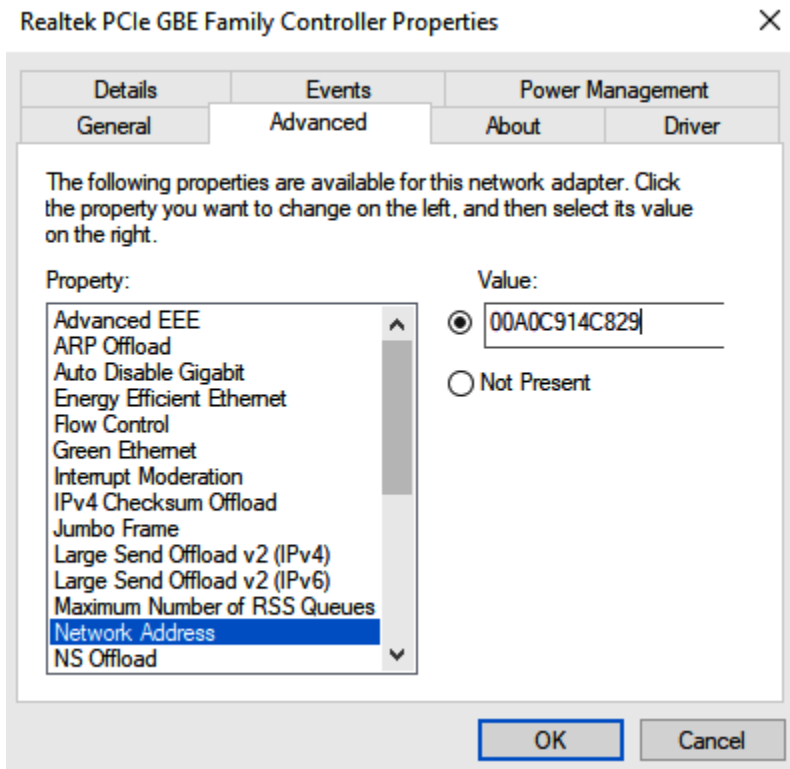
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

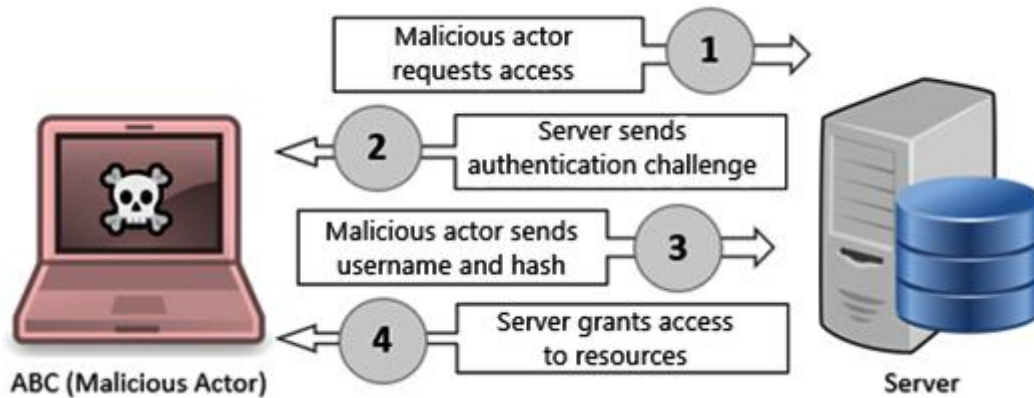
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)



Chapter 10: Protecting Cryptographic Techniques





WEP.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.wep.iv == 0x908422

Number	Time	Source	Destination	Protocol	Info
30	0.0	Apple_3e:91:68	Cisco-Li_4c:bb:74	802.11	Data, SN=31
31	0.0	Apple_3e:91:68	Cisco-Li_4c:bb:74	802.11	Data, SN=31

1

.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_4c:bb:76 (00:1a:70:4c:bb:76)
Transmitter address: Apple_3e:91:68 (e4:ce:8f:3e:91:68)
Destination address: Cisco-Li_4c:bb:74 (00:1a:70:4c:bb:74)
Source address: Apple_3e:91:68 (e4:ce:8f:3e:91:68)
BSS Id: Cisco-Li_4c:bb:76 (00:1a:70:4c:bb:76)
STA address: Apple_3e:91:68 (e4:ce:8f:3e:91:68)
.... 0000 = Fragment number: 0
1100 0110 0110 = Sequence number: 3174

WEP parameters

Initialization Vector: 0x908422 2

Key Index: 0
WEP ICV: 0x0e5acee8 (not verified)

Initialization Vector (wlan.wep.iv), 3 bytes

Packets: 208428 · Displayed: 2 (0.0%) Profile: Default

<http://twitter.com>

Certificate Manager



Your Certificates

Authentication Decisions

People

Servers

Authorities

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
▼ GoDaddy.com, Inc.	
Go Daddy Root Certificate Authority - G2	Builtin Object Token
Go Daddy Secure Certificate Authority - G2	Software Security Device
▼ Google Trust Services LLC	
GTS Root R2	Builtin Object Token
GTS Root R4	Builtin Object Token

View...

Edit Trust...

Import...

Export...

Delete or Distrust...

OK