Protecting Information Assets
- Unit#4c -

Cryptography, Public Key Encryption and Digital Signatures

Cryptography

- Method of transmitting and storing data in a form that only those it is intended for can read and process
- An effective way of protecting sensitive information as it is transmitted through untrusted network communication paths or stored on media

- Complements physical and logical access controls

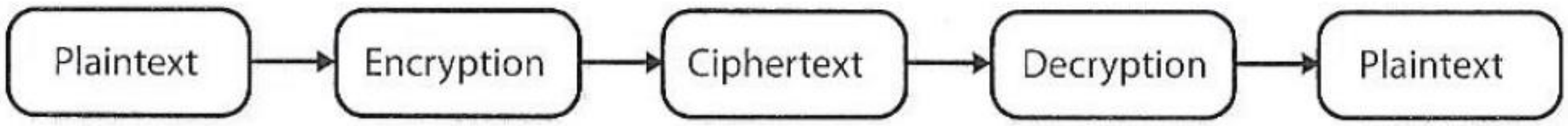
Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

- Kerckhoff's Principle
  - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?

Terminology

- **Plaintext** – is the readable version of a message
- **Ciphertext** – is the unreadable results after an encryption process is applied to the plaintext
- **Cryptosystem** – includes all the necessary components for encryption and decryption
  - Algorithms
  - Keys
  - Software
  - Protocols



Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Cipher = encryption algorithm

2 main attributes combined in a cypher

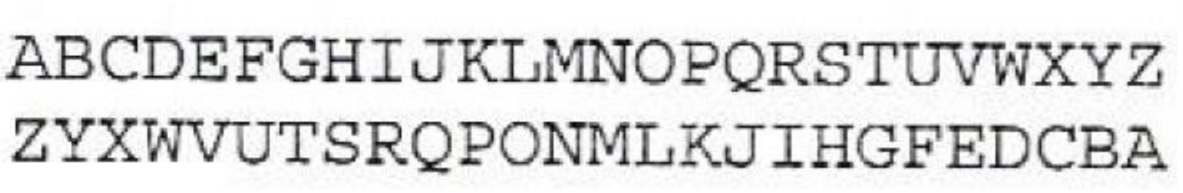
1. **Confusion:** usually carried out through substitution

2. **Diffusion:** Usually carried out through transposition

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Example: Substitution cipher or algorithm

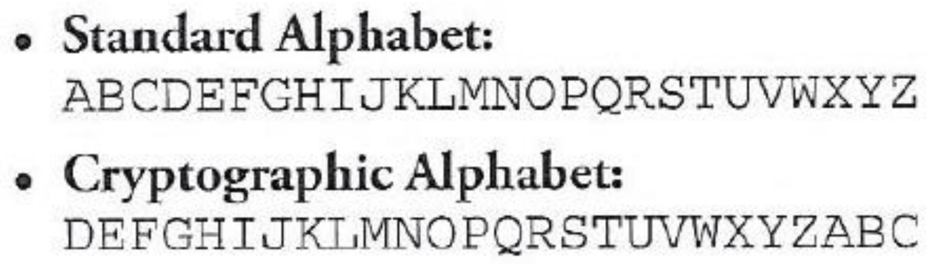
- A mono-alphabetic substitution cipher



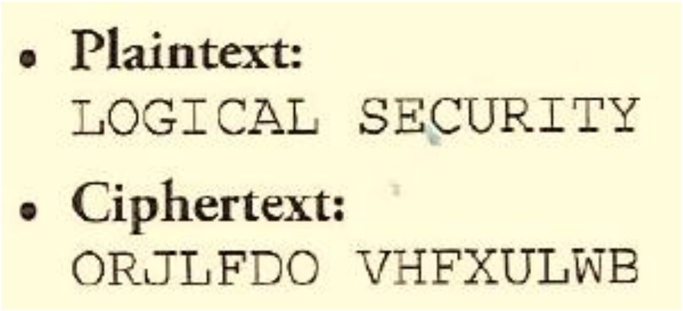
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

“SECURITY” <=> “HVXFIRGB”

- Poly-alphabetic substitution cipher

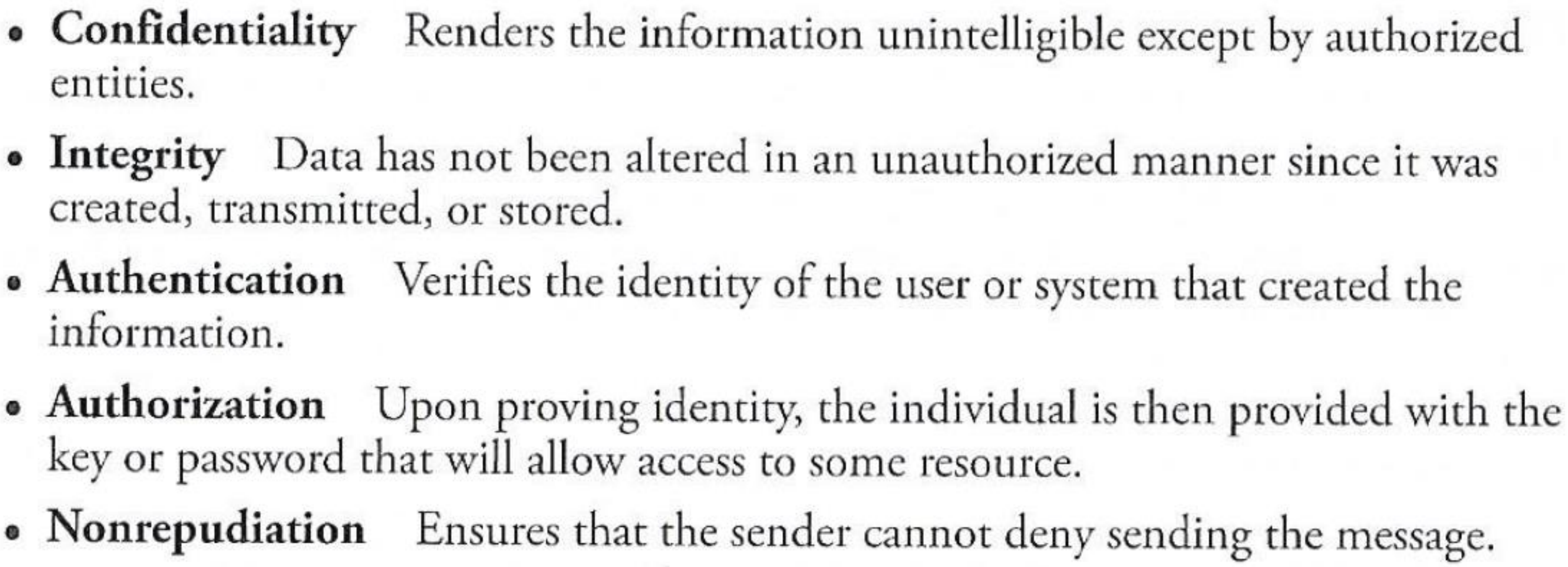


- **Standard Alphabet:**
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
- **Cryptographic Alphabet:**
  DEFGHIJKLMNOPQRSTUVWXYZABC



- **Plaintext:**
  LOGICAL SECURITY
- **Ciphertext:**
  ORJLFDO VHFXULWB

Services of cryptosystems



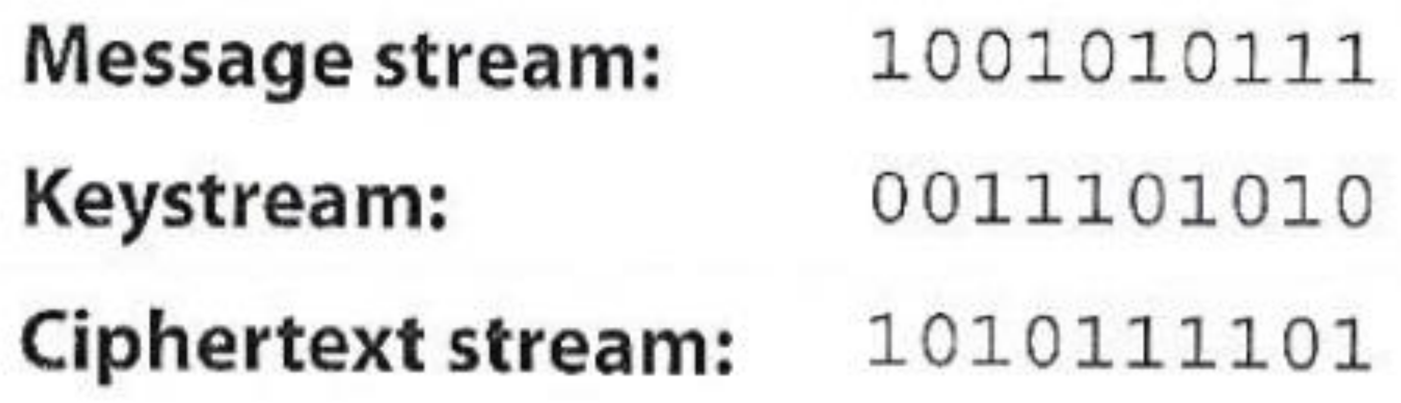
- **Confidentiality** Renders the information unintelligible except by authorized entities.
- **Integrity** Data has not been altered in an unauthorized manner since it was created, transmitted, or stored.
- **Authentication** Verifies the identity of the user or system that created the information.
- **Authorization** Upon proving identity, the individual is then provided with the key or password that will allow access to some resource.
- **Nonrepudiation** Ensures that the sender cannot deny sending the message.

Repudiation – the sender denying he sent the message

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

XOR – Exclusive OR

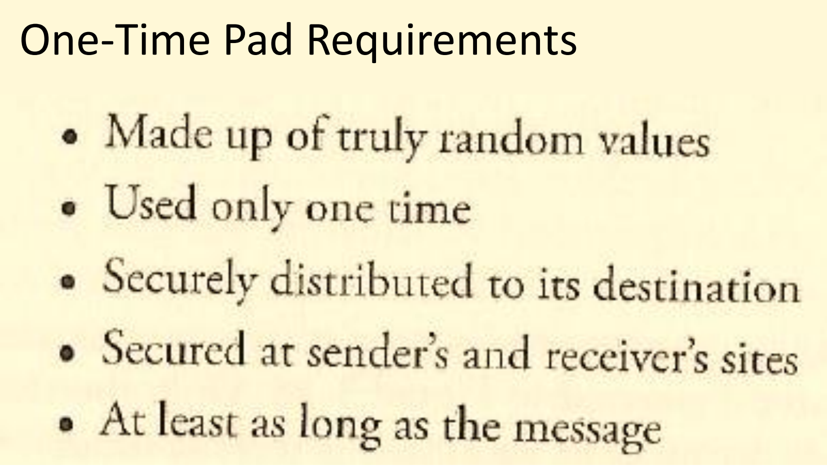
Creating “confusion” through a binary mathematical function called “exclusive OR”, abbreviated as XOR



Message stream:	1001010111
Keystream:	0011101010
Ciphertext stream:	1010111101

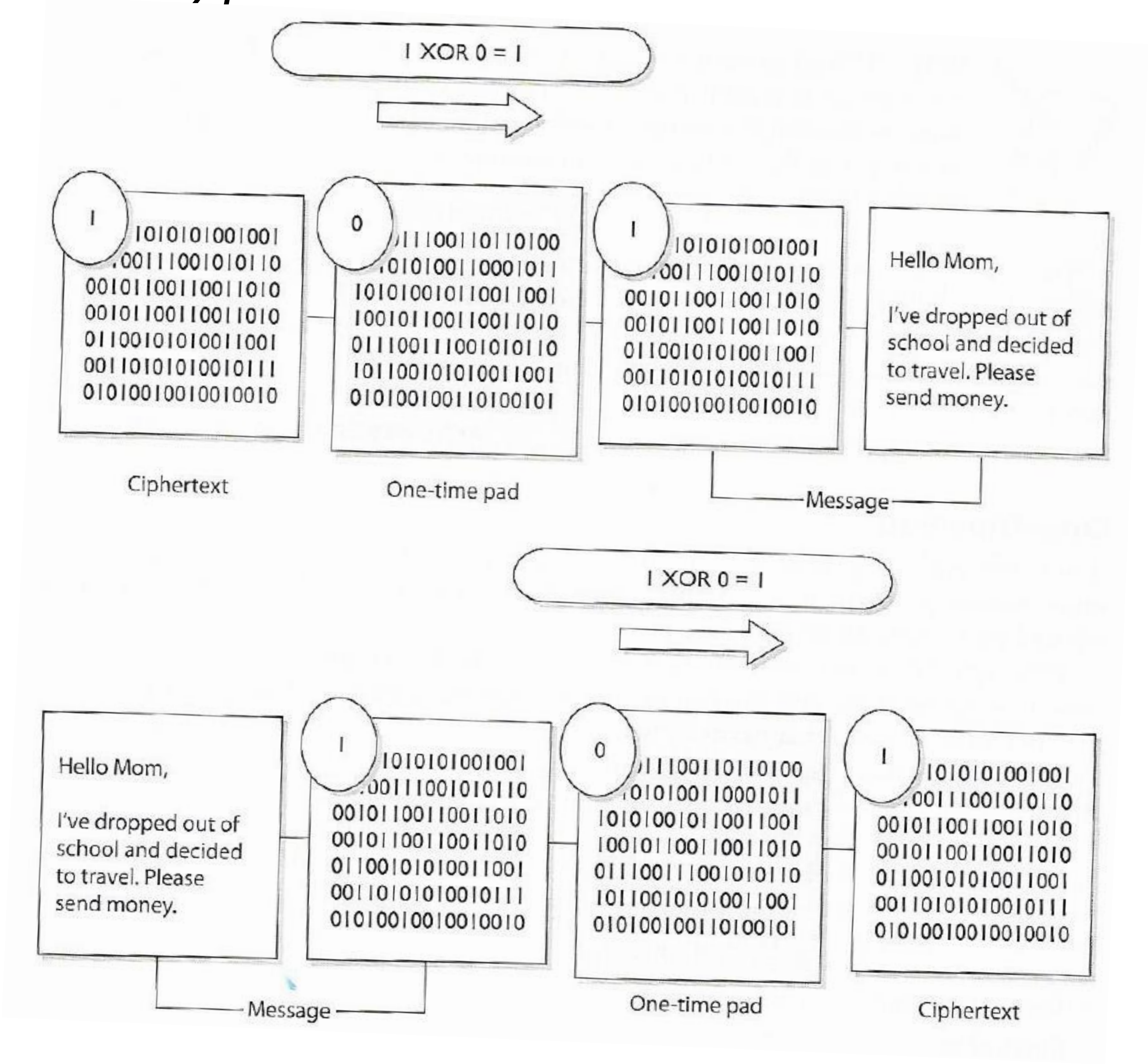
Harris, S. and Maymi, F. (2016) <u>All-In-One CISSP Exam Guide</u>, McGraw Hill Education

One-Time Pad *a perfect encryption scheme*



One-Time Pad Requirements

- Made up of truly random values
- Used only one time
- Securely distributed to its destination
- Secured at sender's and receiver's sites
- At least as long as the message

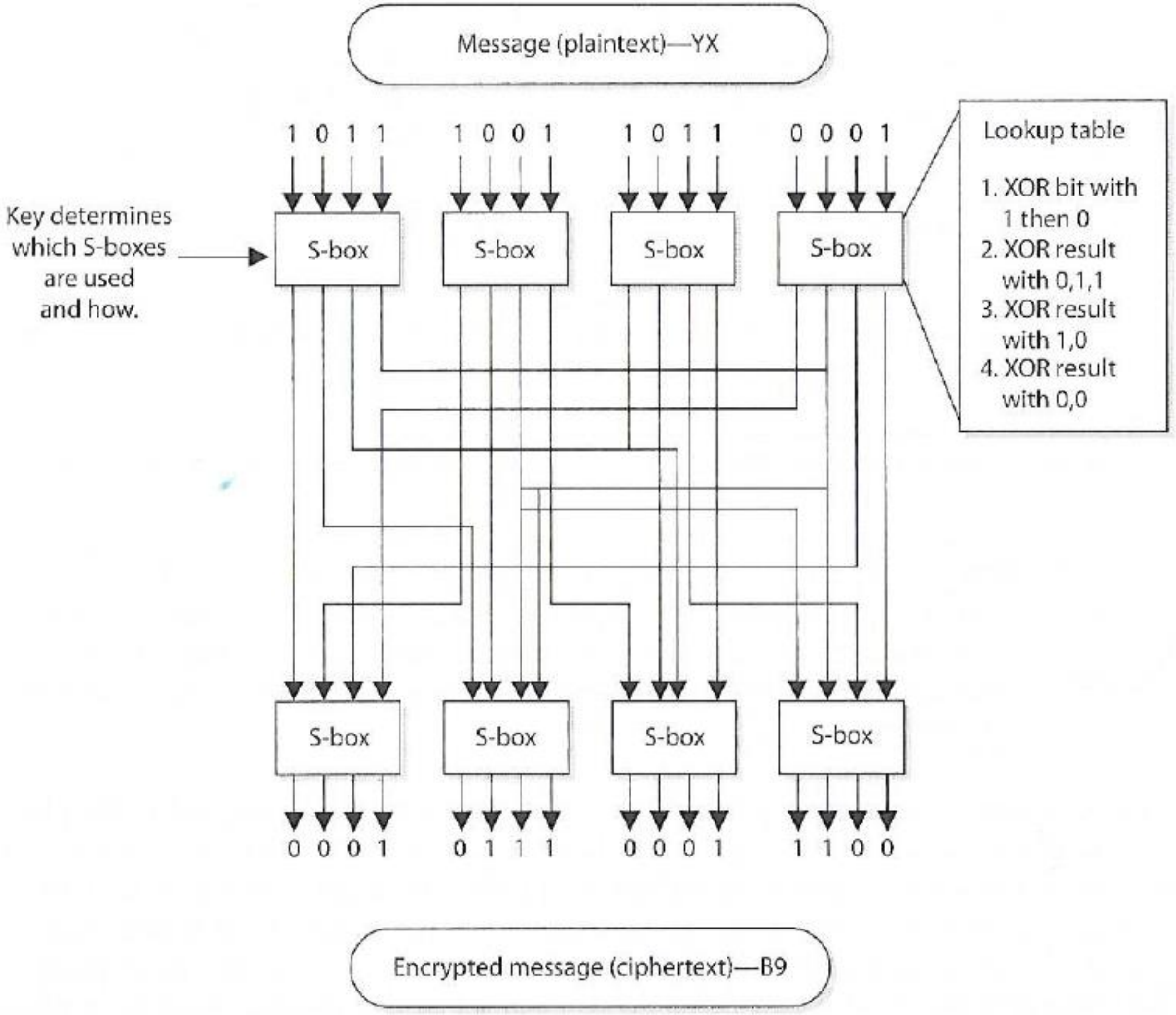


Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

2 main attributes combined in a cypher

1. Confusion: usually carried out through substitution

2. **Diffusion:** Usually carried out through transposition



Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

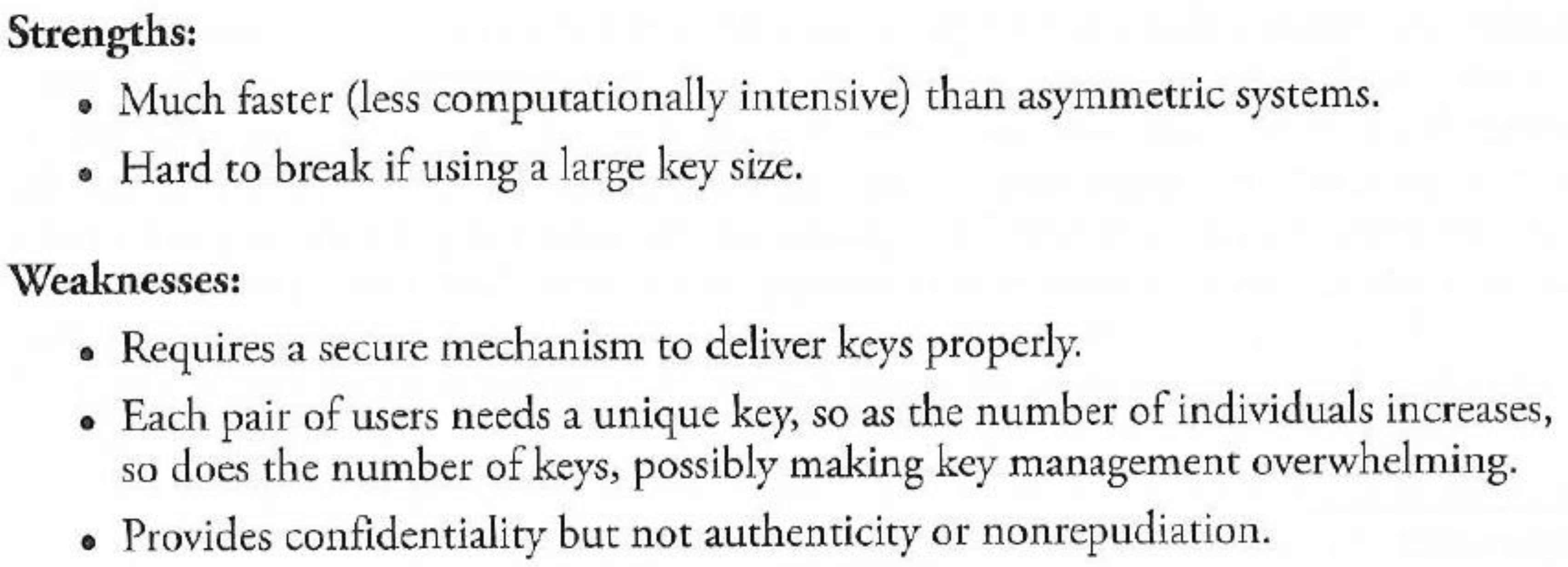
Dichotomies is cryptography

- Symmetric versus Asymmetric
- Stream versus block
- Synchronous versus Asynchronous
- 1-Way functions versus 2-Way functions

Symmetric versus asymmetric algorithms

- Symmetric cryptography
  - Use a copied pair of symmetric (identical) secret keys
  - The sender and the receive use the same key for encryption and decryption functions
- Asymmetric cryptography
  - Also know as “public key cryptography”
  - Use different (“asymmetric”) keys for encryption and decryption
  - One is called the “private key” and the other is the “public key”

Symmetric cryptography



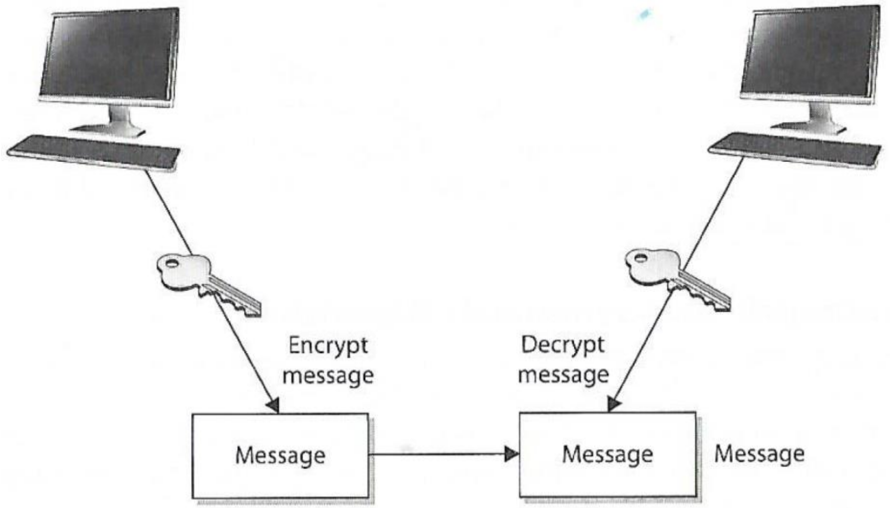
Strengths:

- Much faster (less computationally intensive) than asymmetric systems.
- Hard to break if using a large key size.

Weaknesses:

- Requires a secure mechanism to deliver keys properly.
- Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.
- Provides confidentiality but not authenticity or nonrepudiation.

Symmetric encryption uses the same keys.

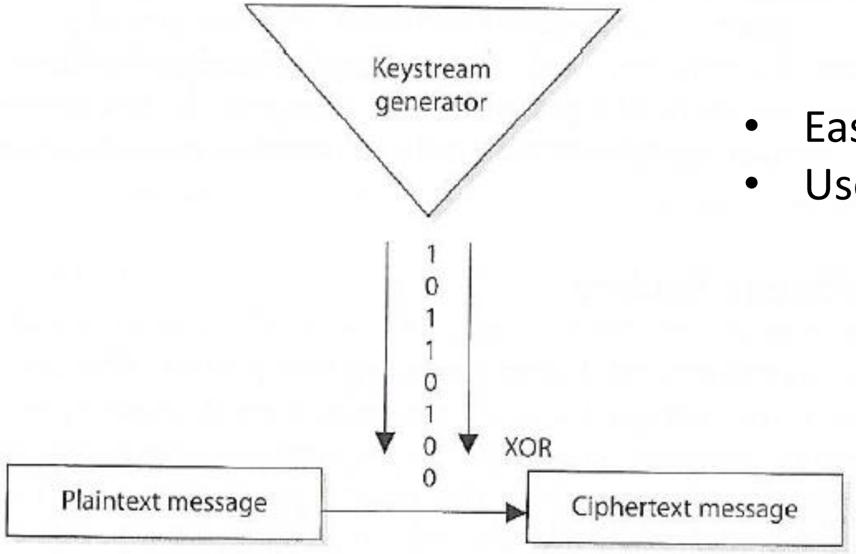


Two types: Stream and Block Ciphers

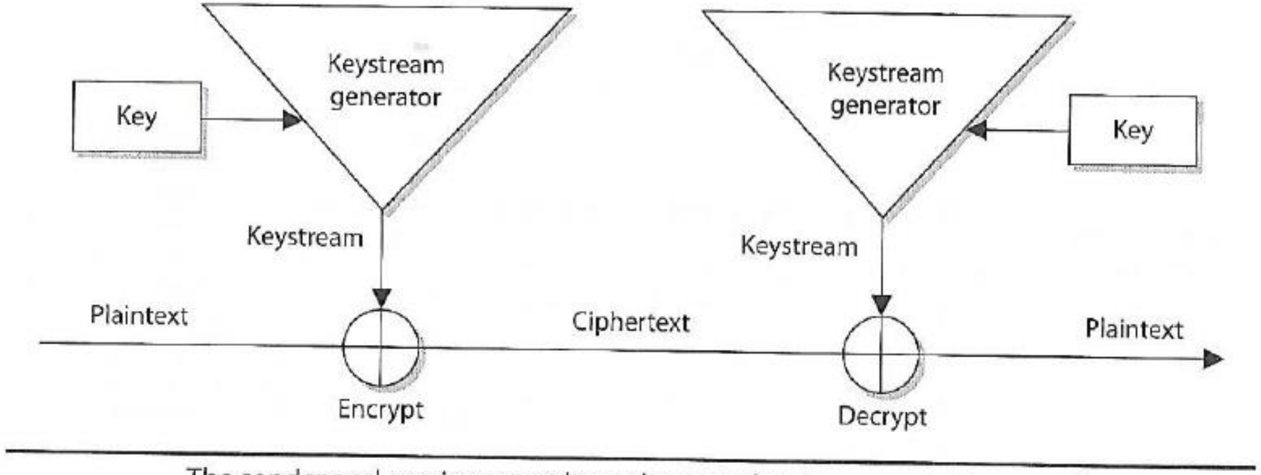
- **Stream Ciphers** treat the message a stream of bits and performs mathematical functions on each bit individually

- **Block Ciphers** divide a message into blocks of bits and transforms the blocks one at a time

Symmetric Stream Ciphers



- Easy to implement in hardware
- Used in cell phones and Voice Over Internet Protocol



The sender and receiver must have the same key to generate the same keystream.

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

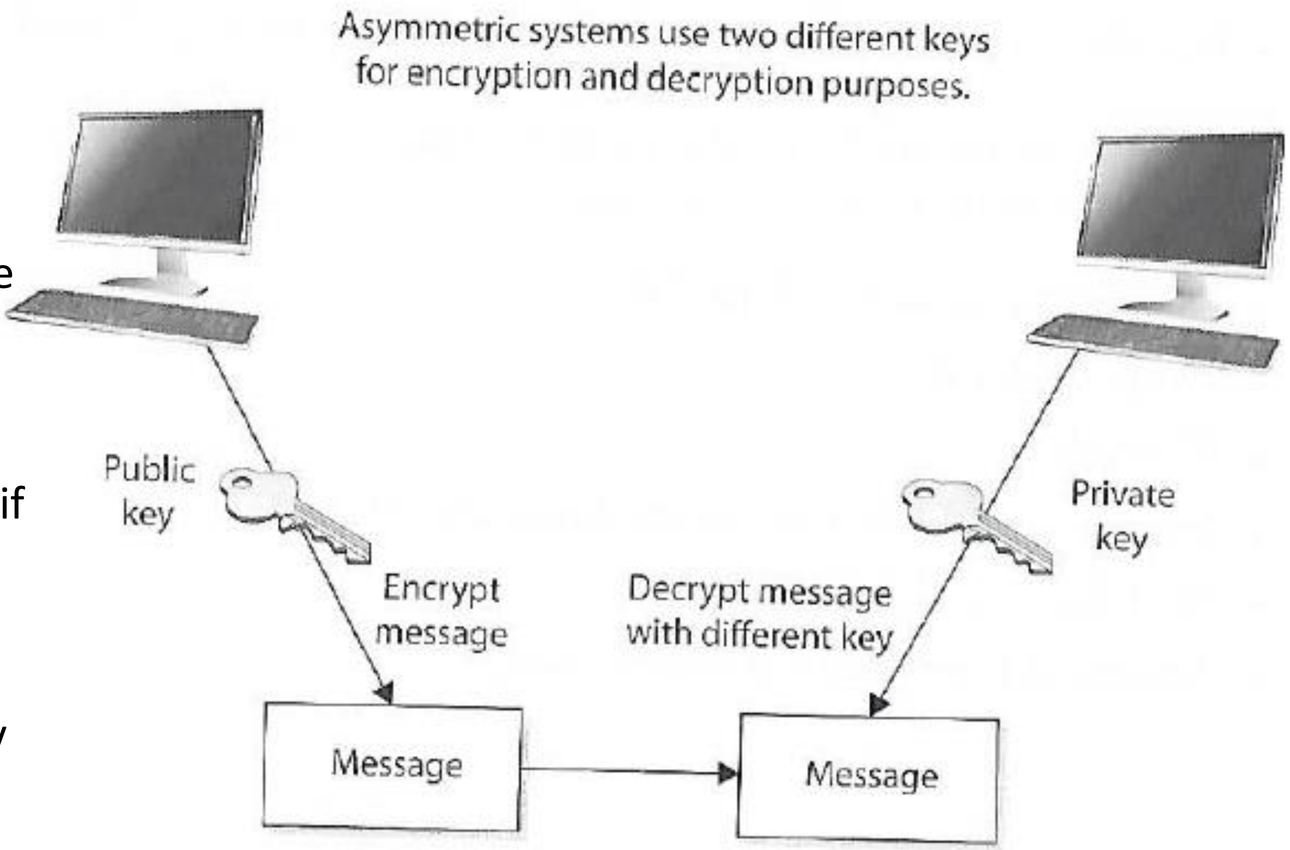
Symmetric versus asymmetric algorithms

- Symmetric cryptography
  - Use a copied pair of symmetric (identical) secret keys
  - The sender and the receive use the same key for encryption and decryption functions
- Asymmetric cryptography
  - Also know as “public key cryptography”
  - Use different (“asymmetric”) keys for encryption and decryption
  - One is called the “private key” and the other is the “public key”

Asymmetric cryptography

- **Public and Private** keys are mathematically related
  - Public keys are generated from private key
  - Private keys cannot be derived from the associated public key (if it falls into the wrong hands)

- **Public key** can be known by everyone
- **Private key** must be known and used only by the owner


Asymmetric systems use two different keys for encryption and decryption purposes.
Public key
Encrypt message
Message
Decrypt message with different key
Private key
Message

Asymmetric cryptography is computational intensive and much slower than symmetric cryptography

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Asymmetric cryptography

- Do not get confused and think the public key is only for encryption and private key is only for decryption!

- Each key type can be use used to encrypt and decrypt
  - If data is encrypted with a private key it cannot be decrypted with the same private key (but it can be decrypted with the related public key)
  - If data is encrypted with a public key it cannot be decrypted with the same public key (but it can be decrypted with the related private key)

Asymmetric cryptography

If the sender (“Jill”) encrypts data with her private key, the receiver (“Bill”) must have a copy of Jill’s public key to decrypt it

- By decrypting the message with Jill’s public key Bill can be sure the message really came from Jill
- A message can be decrypted with a public key only if the message was encrypted with the corresponding private key
  - *This provides **authentication** because Jill is only the only one who is supposed to have her private key*

If Bill (the receiver) wants to make sure Jill is the only one who can read his reply, he will encrypt the response with her public key

– *Only Jill will be able to decrypt the message, because she is the only one who has the necessary private key*

– *This provides **confidentiality** because only Jill is able to decrypt the message with her private key*

Asymmetric cryptography

Why would Bill (now the sender) choose to encrypt his reply to Jill with his private key instead of using Jill’s public key?

- **Authentication** – Bill wants Jill to know that the message came from him and no one else
- If he encrypted the data with Jill’s public key, it does not provide authenticity because anyone can get Jill’s public key
- If he uses his private key to encrypt the data, then Jill can be sure the message came from him and no one else

Note: *Symmetric keys do not provide authenticity – because the same key is used on both ends (using one of the secret keys does not ensure the message originated from a specific individual*

Asymmetric cryptography

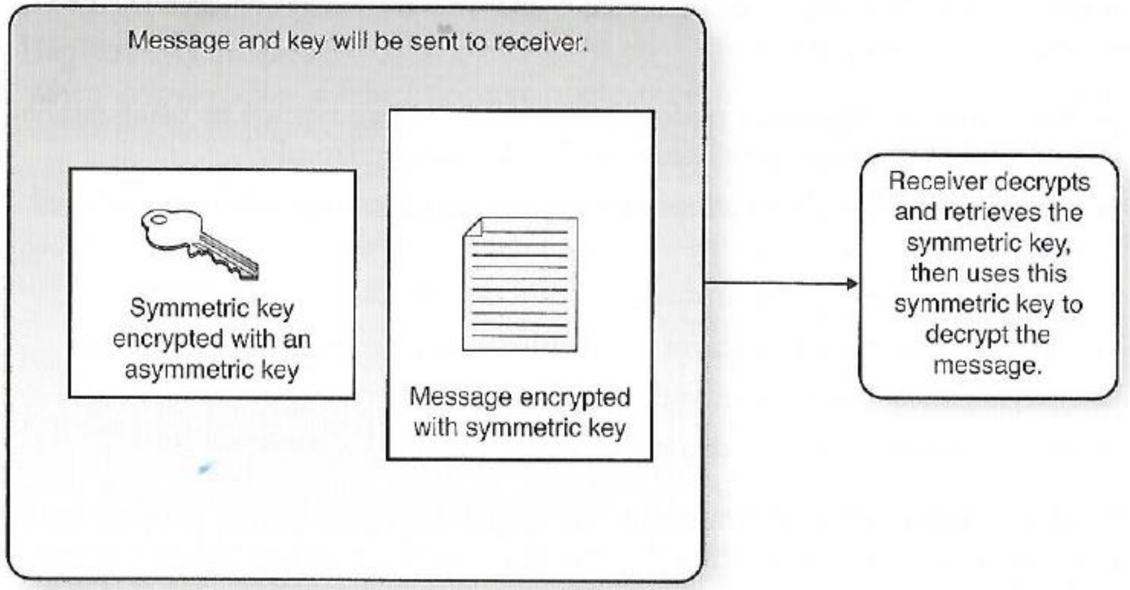
- If **confidentiality** is the most important security service, the sender would encrypt the file with the receiver’s public key
  - This is called a “**secure message format**” because it can only be decrypted by the person with the corresponding private key

- If **authentication** is most important, the sender would encrypt the data with his private key
  - This provides assurance to the receiver that the only person who could have encrypted the data is the individual in possession of the private key
  - If the sender encrypted the data with receivers public key, authentication is not provided because the public key is available to anyone
  - Encrypting data with the senders private key is called an “**open message format**” because anyone with a copy of the corresponding public key can decrypt the message
  - Confidentiality is not assured

Hybrid Encryption (a.k.a. “digital envelope”)

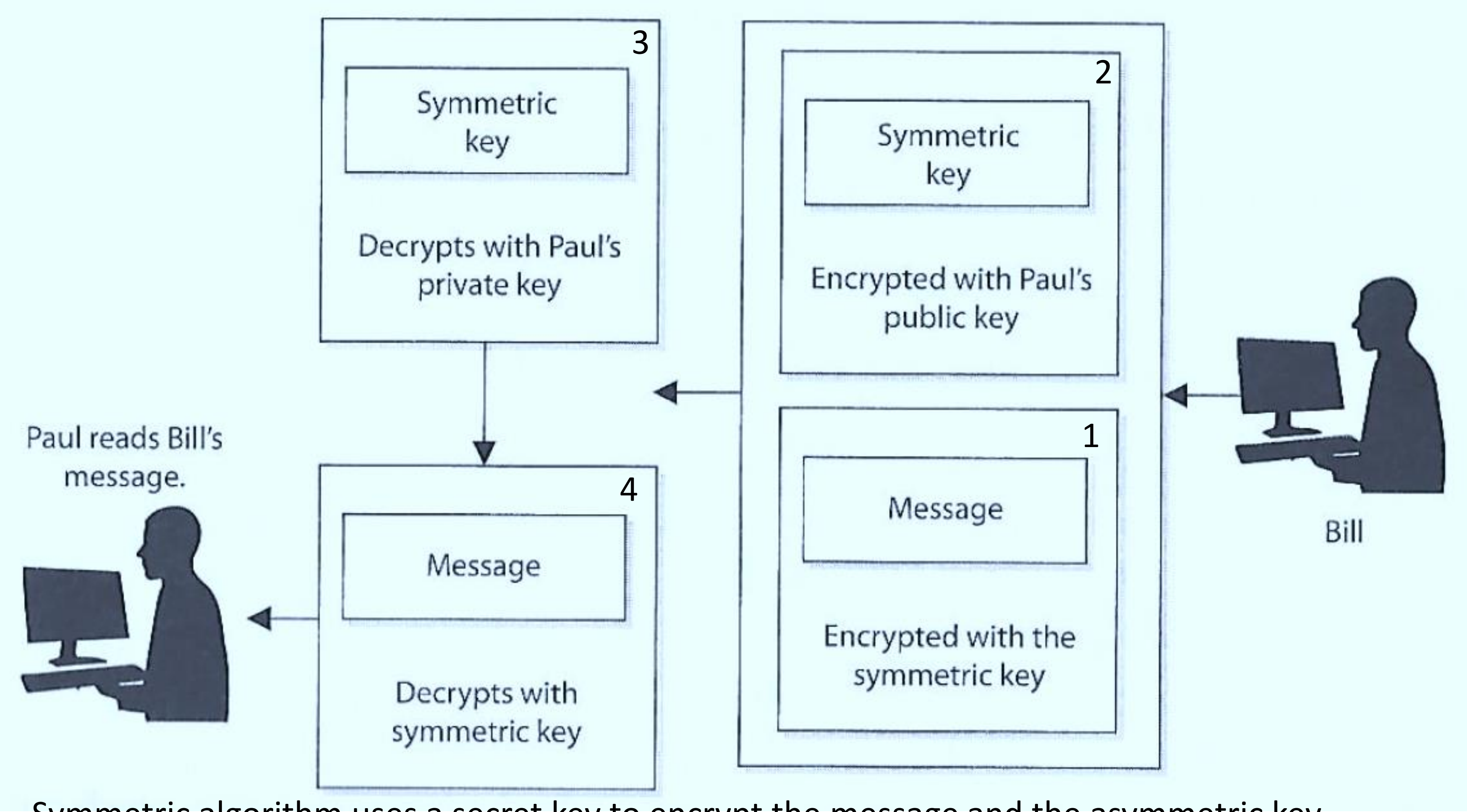
Symmetric and asymmetric and algorithms are often used together

- Public key cryptography’s asymmetric algorithm is used to create public and private keys for secure automated key distribution
- Symmetric algorithm is used to create secret keys for rapid encryption/decryption of bulk data


Message and key will be sent to receiver.
Symmetric key encrypted with an asymmetric key
Message encrypted with symmetric key
Receiver decrypts and retrieves the symmetric key, then uses this symmetric key to decrypt the message.

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Hybrid Encryption


3
Symmetric key
Decrypts with Paul's private key
2
Symmetric key
Encrypted with Paul's public key
Paul reads Bill's message.
1
Message
Encrypted with the symmetric key
Bill
4
Message
Decrypts with symmetric key

Symmetric algorithm uses a secret key to encrypt the message and the asymmetric key encrypts the secret key for transmission (SSL/TLS uses hybrid)

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Quick review

1. If a symmetric key is encrypted with a receiver’s public key, what security service is provided?

Quick review

1. If a symmetric key is encrypted with a receiver’s public key, what security service is provided?
    - **Confidentiality**: only the receiver’s private key can be used to decrypt the symmetric key, and only the receiver should have access to this private key

Quick review

2. If data is encrypted with the sender’s private key, what security services is provided?

Quick review

2. If data is encrypted with the sender’s private key, what security services are provided?
    - **Authenticity** of the sender and nonrepudiation. If the receiver can decrypt the encrypted data with the sender’s public key, then receiver knows the data was encrypted with the sender’s private key

Quick review

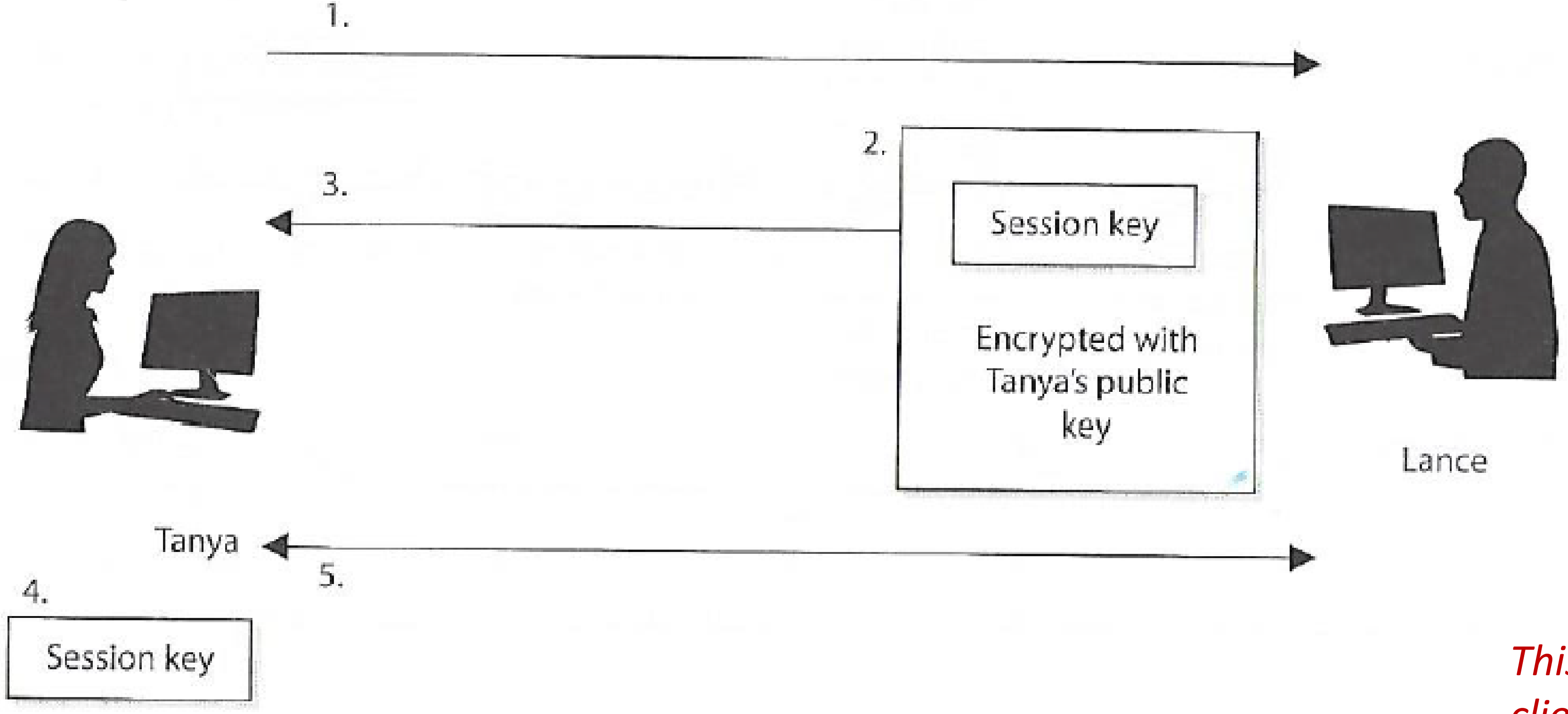
3. Why do we encrypt the message with the symmetric key rather than the asymmetric key?

Quick review

3. Why do we encrypt the message with the symmetric key rather than the asymmetric key?
    - **Because the asymmetric key algorithm is too slow**

Session keys

Single-use symmetric keys used to encrypt messages between two users in an individual communication session



1) Tanya sends Lance her public key.
2) Lance generates a random session key and encrypts it using Tanya's public key.
3) Lance sends the session key, encrypted with Tanya's public key, to Tanya.
4) Tanya decrypts Lance's message with her private key and now has a copy of the session key.
5) Tanya and Lance use this session key to encrypt and decrypt messages to each other.

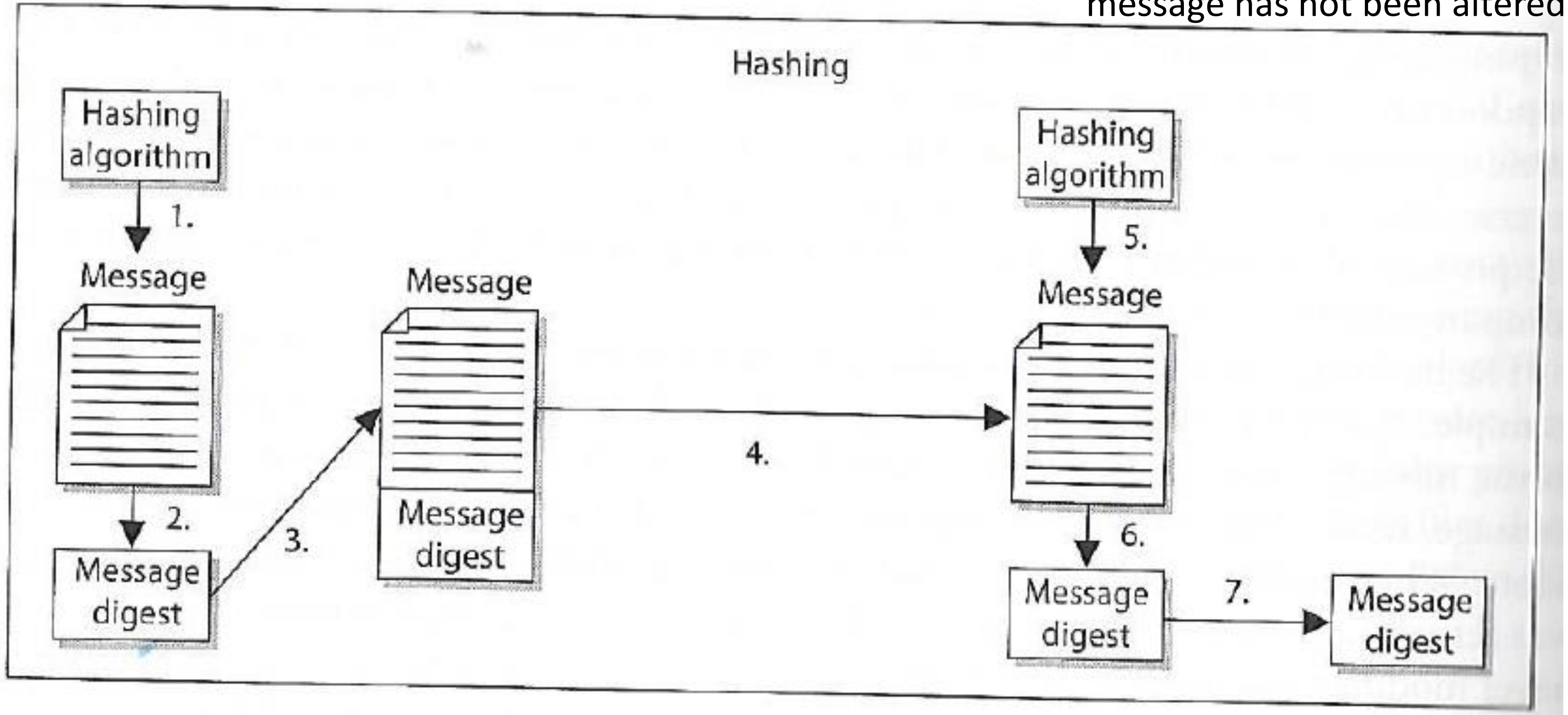
This is how secure web client applications communicate with server-side services

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

One-way Hash

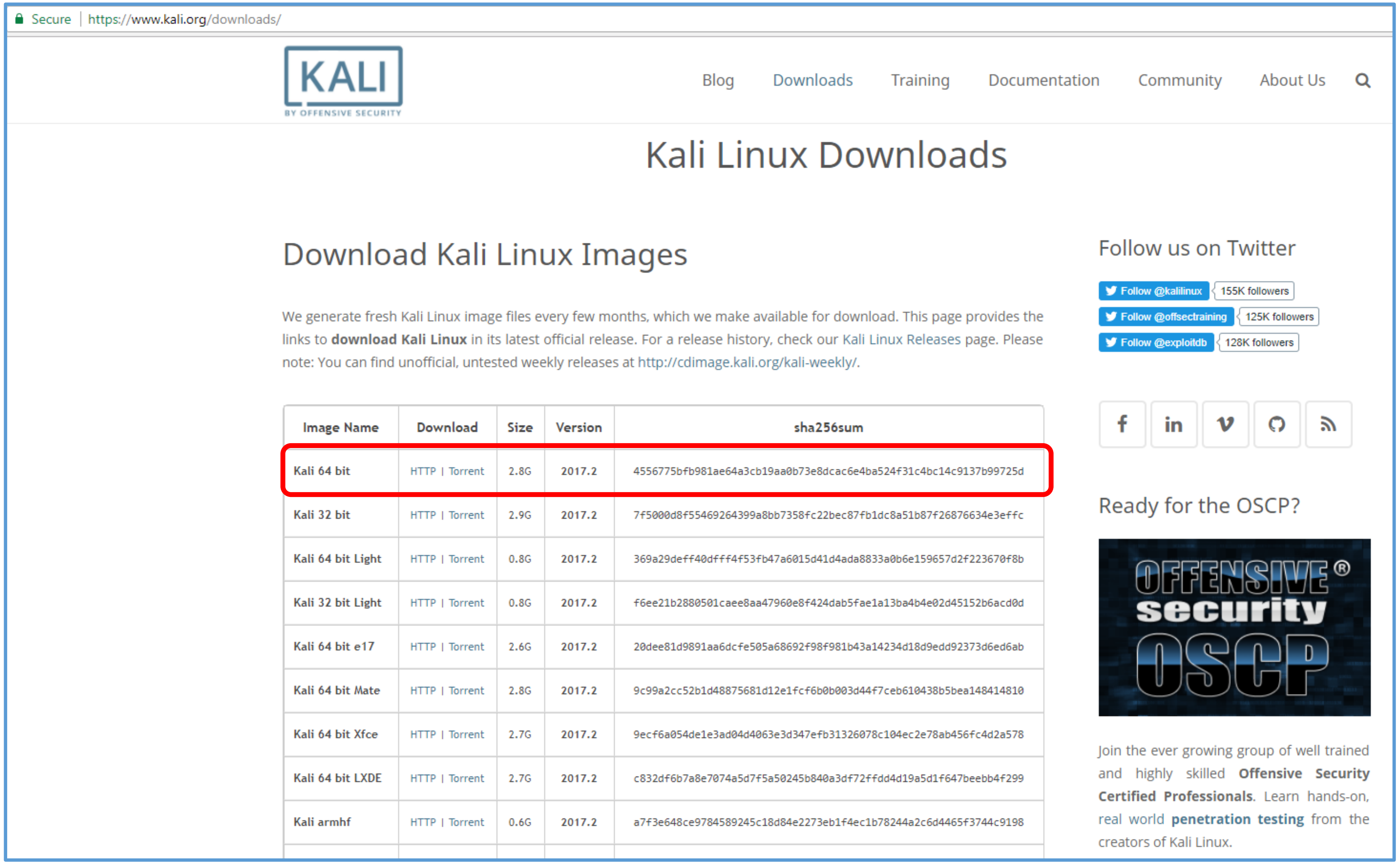
- Assures message **integrity**
- A function that takes a variable-length string (i.e. message) and produces a fixed-length value called a hash value
- Does not use keys

1. Sender puts message through hashing function
2. Message digest generated
3. Message digest appended to the message
4. Sender sends message to receiver
5. Receiver puts message through hashing function
6. Receiver generates message digest value
7. Receiver compares the two message digests values. If they are the same, the message has not been altered



One-way hash example…

Testing the integrity of a file (e.g. program) downloaded from the internet…


Secure | https://www.kali.org/downloads/
KALI
BY OFFENSIVE SECURITY
Blog
Downloads
Training
Documentation
Community
About Us
Follow @kalilinux 155K followers
Follow @offsectraining 125K followers
Follow @exploitdb 128K followers
OFFENSIVE® security OSCP

Kali Linux Downloads

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to **download Kali Linux** in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/.

Image Name	Download	Size	Version	sha256sum
Kali 64 bit	HTTP | Torrent	2.8G	2017.2	4556775bfb981ae64a3cb19aa0b73e8dcac6e4ba524f31c4bc14c9137b99725d
Kali 32 bit	HTTP | Torrent	2.9G	2017.2	7f5000d8f55469264399a8bb7358fc22bec87fb1dc8a51b87f26876634e3effc
Kali 64 bit Light	HTTP | Torrent	0.8G	2017.2	369a29deff40dfff4f53fb47a6015d41d4ada8833a0b6e159657d2f223670f8b
Kali 32 bit Light	HTTP | Torrent	0.8G	2017.2	f6ee21b2880501caee8aa47960e8f424dab5fae1a13ba4b4e02d45152b6acd0d
Kali 64 bit e17	HTTP | Torrent	2.6G	2017.2	20dee81d9891aa6dcfe505a68692f98f981b43a14234d18d9edd92373d6ed6ab
Kali 64 bit Mate	HTTP | Torrent	2.8G	2017.2	9c99a2cc52b1d48875681d12e1fcf6b0b003d44f7ceb610438b5bea148414810
Kali 64 bit Xfce	HTTP | Torrent	2.7G	2017.2	9ecf6a054de1e3ad04d4063e3d347efb31326078c104ec2e78ab456fc4d2a578
Kali 64 bit LXDE	HTTP | Torrent	2.7G	2017.2	c832df6b7a8e7074a5d7f5a50245b840a3df72ffdd4d19a5d1f647beebb4f299
Kali armhf	HTTP | Torrent	0.6G	2017.2	a7f3e648ce9784589245c18d84e2273eb1f4ec1b78244a2c6d4465f3744c9198

Follow us on Twitter

Ready for the OSCP?

Join the ever growing group of well trained and highly skilled **Offensive Security Certified Professionals**. Learn hands-on, real world **penetration testing** from the creators of Kali Linux.

One-way hash example…

Testing the integrity of a file (e.g. program) from the internet…

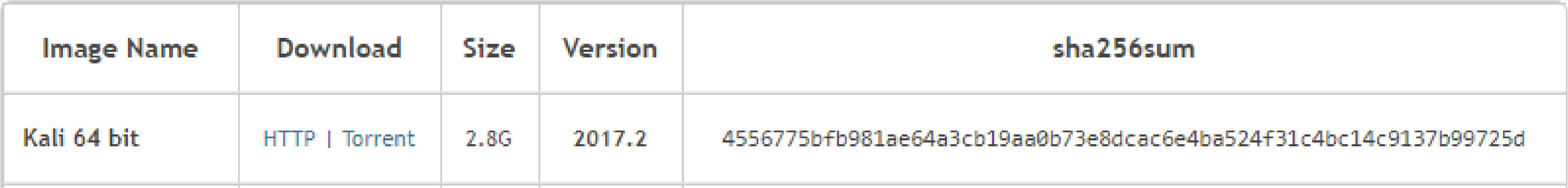
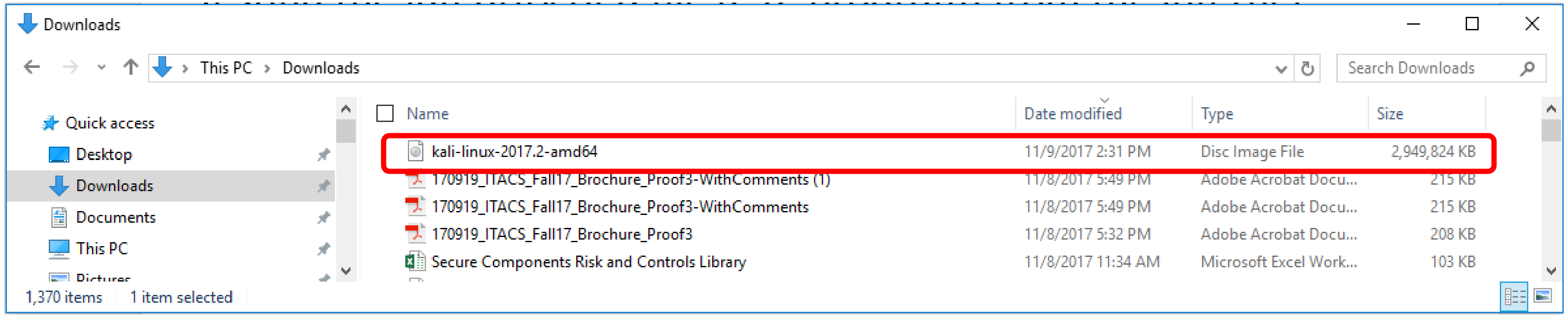


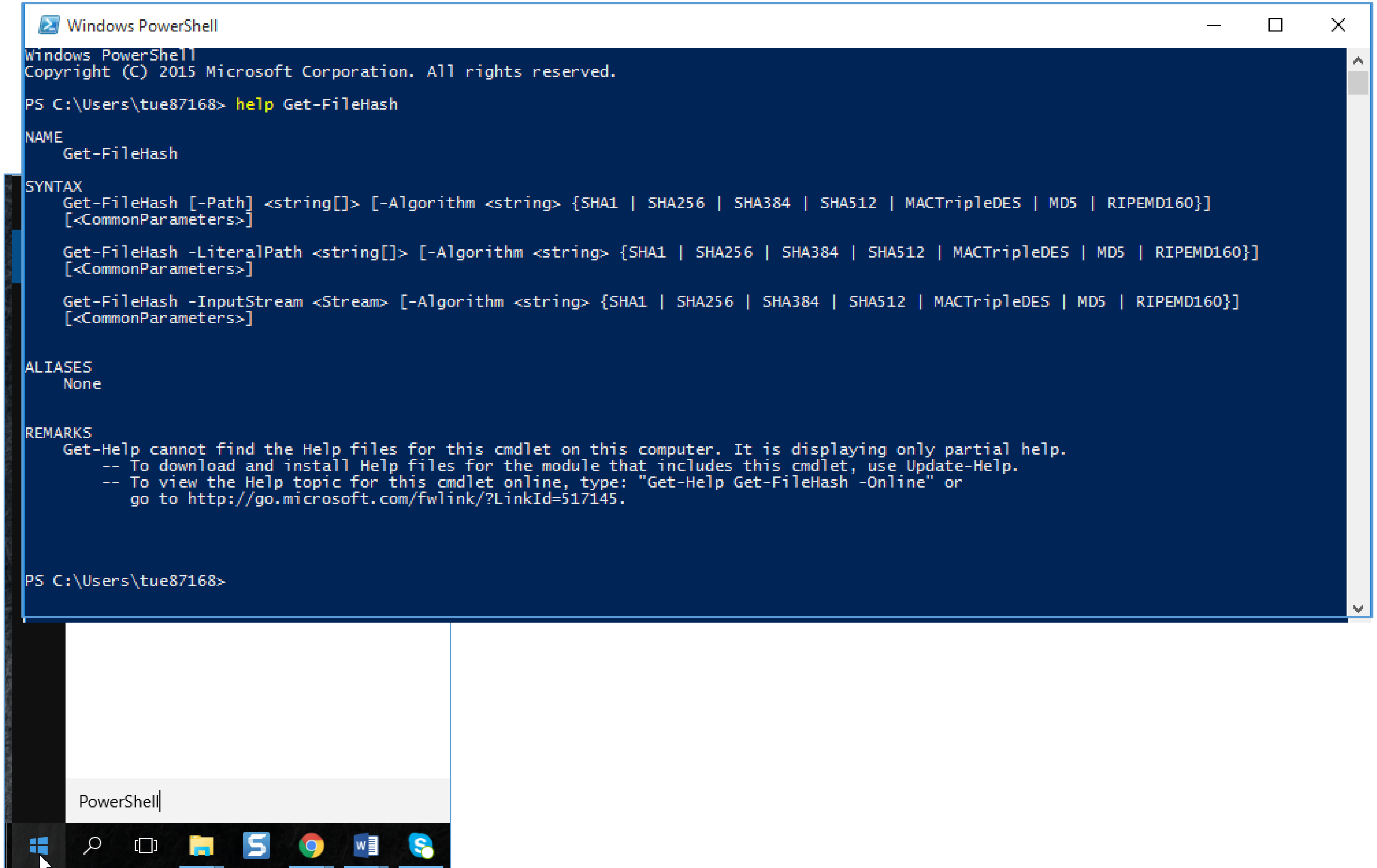
Image Name	Download	Size	Version	sha256sum
Kali 64 bit	HTTP | Torrent	2.8G	2017.2	4556775bfb981ae64a3cb19aa0b73e8dcac6e4ba524f31c4bc14c9137b99725d



Name	Date modified	Type	Size
kali-linux-2017.2-amd64	11/9/2017 2:31 PM	Disc Image File	2,949,824 KB
170919_ITACS_Fall17_Brochure_Proof3-WithComments (1)	11/8/2017 5:49 PM	Adobe Acrobat Docu...	215 KB
170919_ITACS_Fall17_Brochure_Proof3-WithComments	11/8/2017 5:49 PM	Adobe Acrobat Docu...	215 KB
170919_ITACS_Fall17_Brochure_Proof3	11/8/2017 5:32 PM	Adobe Acrobat Docu...	208 KB
Secure Components Risk and Controls Library	11/8/2017 11:34 AM	Microsoft Excel Work...	103 KB

Is the Kali I downloaded the same Kali that was published?

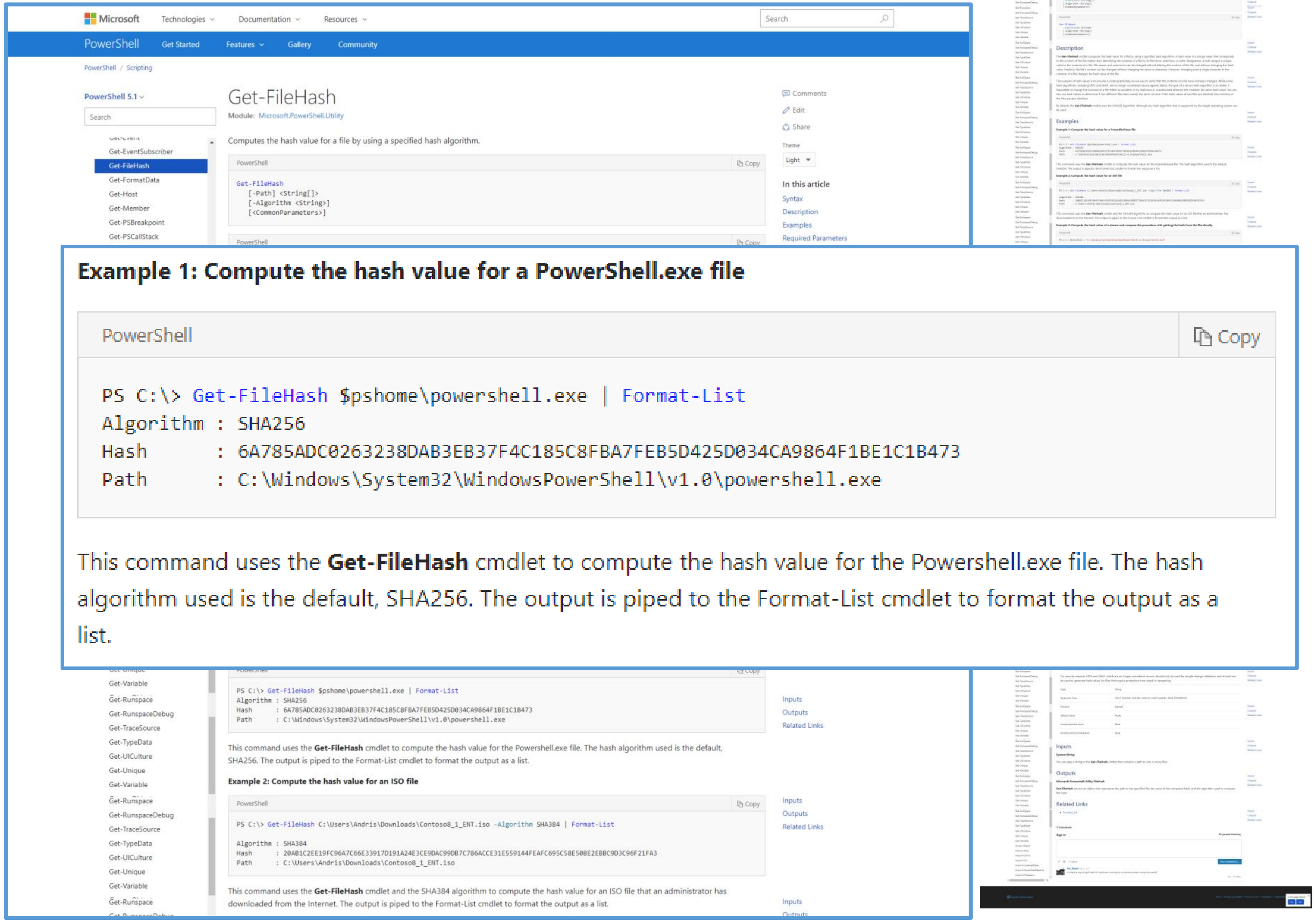
One-way hash example…



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\tue87168> help Get-FileHash

NAME
    Get-FileHash

SYNTAX
    Get-FileHash [-Path] <string[]> [-Algorithm <string> {SHA1 | SHA256 | SHA384 | SHA512 | MACTripleDES | MD5 | RIPEMD160}]
    [<CommonParameters>]

    Get-FileHash -LiteralPath <string[]> [-Algorithm <string> {SHA1 | SHA256 | SHA384 | SHA512 | MACTripleDES | MD5 | RIPEMD160}]
    [<CommonParameters>]

    Get-FileHash -InputStream <Stream> [-Algorithm <string> {SHA1 | SHA256 | SHA384 | SHA512 | MACTripleDES | MD5 | RIPEMD160}]
    [<CommonParameters>]


ALIASES
    None


REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
        -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
        -- To view the Help topic for this cmdlet online, type: "Get-Help Get-FileHash -Online" or
           go to http://go.microsoft.com/fwlink/?LinkId=517145.



PS C:\Users\tue87168>
```

One-way hash example…

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-5.1



Get-FileHash

Module: Microsoft.PowerShell.Utility

Computes the hash value for a file by using a specified hash algorithm.

PowerShell

```
Get-FileHash
   [-Path] <String[]>
   [-Algorithm <String>]
   [<CommonParameters>]
```

Example 1: Compute the hash value for a PowerShell.exe file

PowerShell   Copy

```
PS C:\> Get-FileHash $pshome\powershell.exe | Format-List
Algorithm : SHA256
Hash      : 6A785ADC0263238DAB3EB37F4C185C8FBA7FEB5D425D034CA9864F1BE1C1B473
Path      : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

This command uses the **Get-FileHash** cmdlet to compute the hash value for the Powershell.exe file. The hash algorithm used is the default, SHA256. The output is piped to the Format-List cmdlet to format the output as a list.

```
PS C:\> Get-FileHash $pshome\powershell.exe | Format-List
Algorithm : SHA256
Hash      : 6A785ADC0263238DAB3EB37F4C185C8FBA7FEB5D425D034CA9864F1BE1C1B473
Path      : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

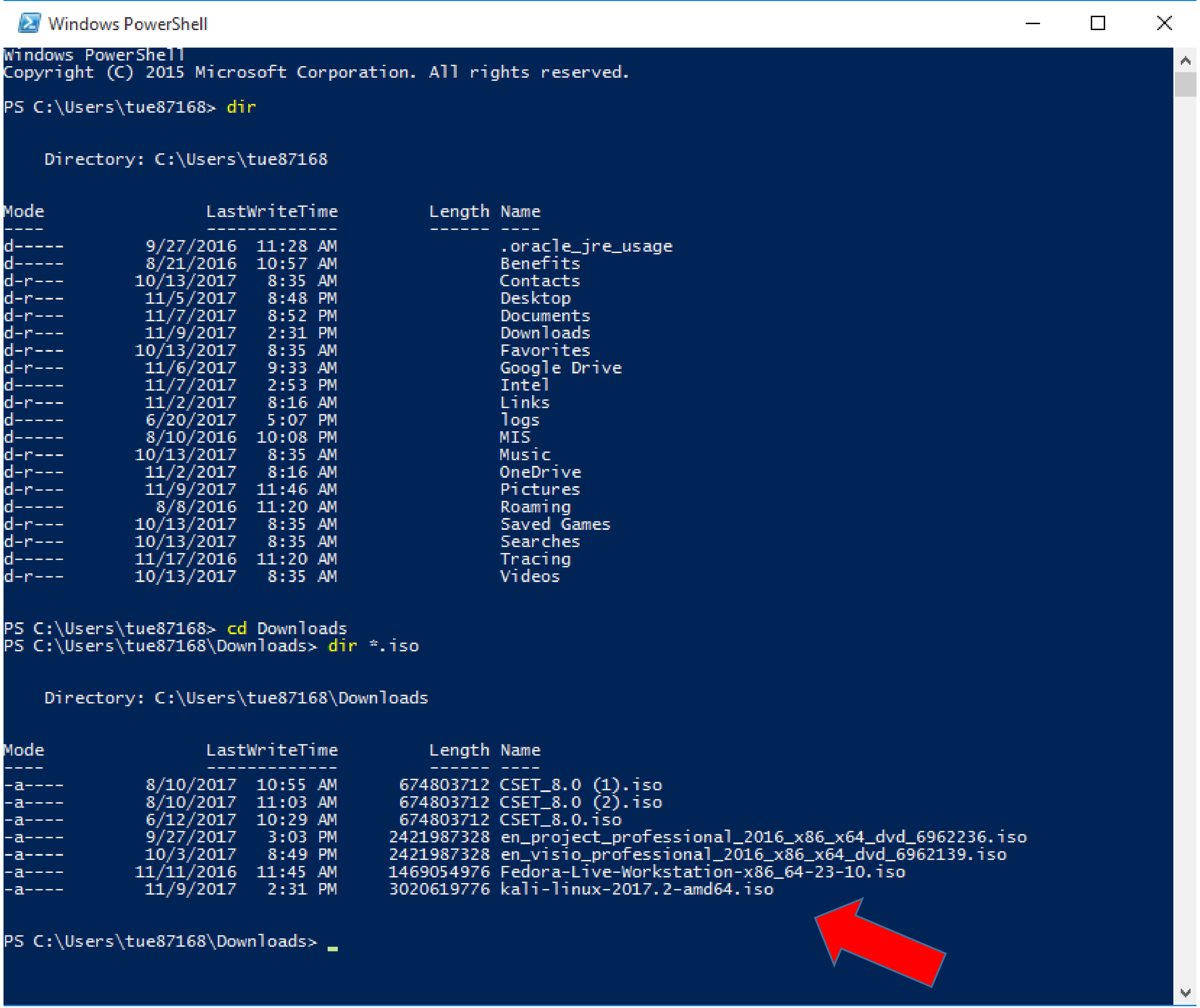
This command uses the **Get-FileHash** cmdlet to compute the hash value for the Powershell.exe file. The hash algorithm used is the default, SHA256. The output is piped to the Format-List cmdlet to format the output as a list.

Example 2: Compute the hash value for an ISO file

PowerShell   Copy

```
PS C:\> Get-FileHash C:\Users\Andris\Downloads\Contoso8_1_ENT.iso -Algorithm SHA384 | Format-List

Algorithm : SHA384
Hash      : 20AB1C2EE19FC96A7C66E33917D191A24E3CE9DAC99DB7C786ACCE31E559144FEAFC695C58E508E2EBBC9D3C96F21FA3
Path      : C:\Users\Andris\Downloads\Contoso8_1_ENT.iso
```

This command uses the **Get-FileHash** cmdlet and the SHA384 algorithm to compute the hash value for an ISO file that an administrator has downloaded from the Internet. The output is piped to the Format-List cmdlet to format the output as a list.



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\tue87168> dir


    Directory: C:\Users\tue87168


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        9/27/2016  11:28 AM                .oracle_jre_usage
d-----        8/21/2016  10:57 AM                Benefits
d-r---       10/13/2017   8:35 AM                Contacts
d-r---        11/5/2017   8:48 PM                Desktop
d-r---        11/7/2017   8:52 PM                Documents
d-r---        11/9/2017   2:31 PM                Downloads
d-r---       10/13/2017   8:35 AM                Favorites
d-r---        11/6/2017   9:33 AM                Google Drive
d-----        11/7/2017   2:53 PM                Intel
d-r---        11/2/2017   8:16 AM                Links
d-----        6/20/2017   5:07 PM                logs
d-----        8/10/2016  10:08 PM                MIS
d-r---       10/13/2017   8:35 AM                Music
d-r---        11/2/2017   8:16 AM                OneDrive
d-r---        11/9/2017  11:46 AM                Pictures
d-----         8/8/2016  11:20 AM                Roaming
d-r---       10/13/2017   8:35 AM                Saved Games
d-r---       10/13/2017   8:35 AM                Searches
d-----       11/17/2016  11:20 AM                Tracing
d-r---       10/13/2017   8:35 AM                Videos


PS C:\Users\tue87168> cd Downloads
PS C:\Users\tue87168\Downloads> dir *.iso


    Directory: C:\Users\tue87168\Downloads


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        8/10/2017  10:55 AM      674803712 CSET_8.0 (1).iso
-a----        8/10/2017  11:03 AM      674803712 CSET_8.0 (2).iso
-a----        6/12/2017  10:29 AM      674803712 CSET_8.0.iso
-a----        9/27/2017   3:03 PM     2421987328 en_project_professional_2016_x86_x64_dvd_6962236.iso
-a----        10/3/2017   8:49 PM     2421987328 en_visio_professional_2016_x86_x64_dvd_6962139.iso
-a----       11/11/2016  11:45 AM     1469054976 Fedora-Live-Workstation-x86_64-23-10.iso
-a----        11/9/2017   2:31 PM     3020619776 kali-linux-2017.2-amd64.iso


PS C:\Users\tue87168\Downloads> _
```

One-way hash example…

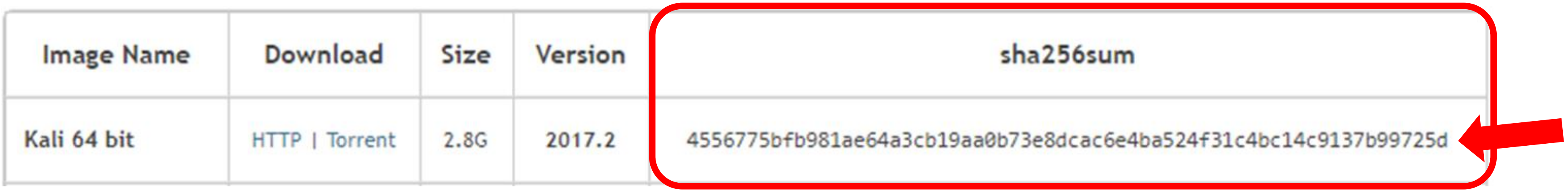
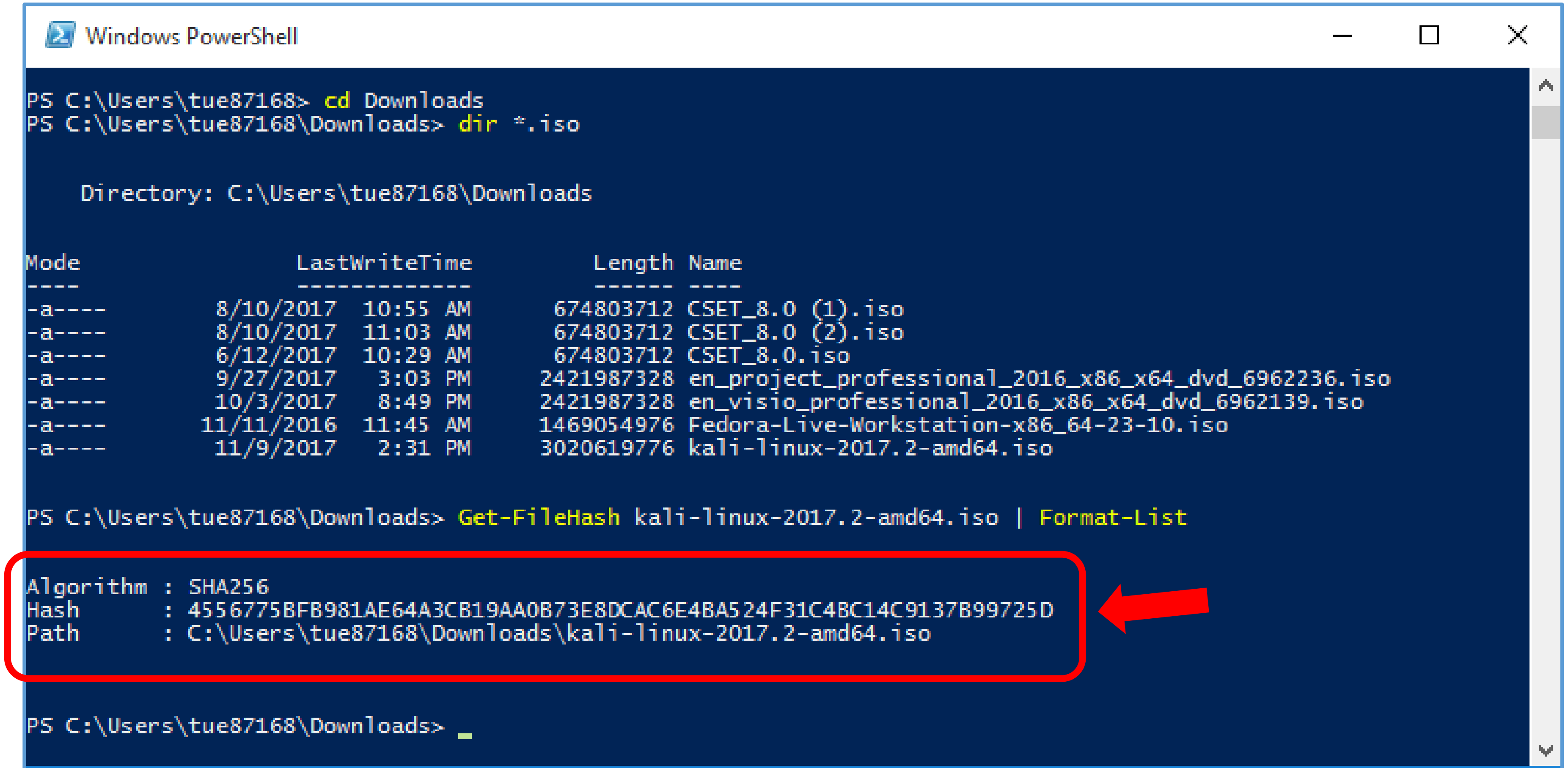
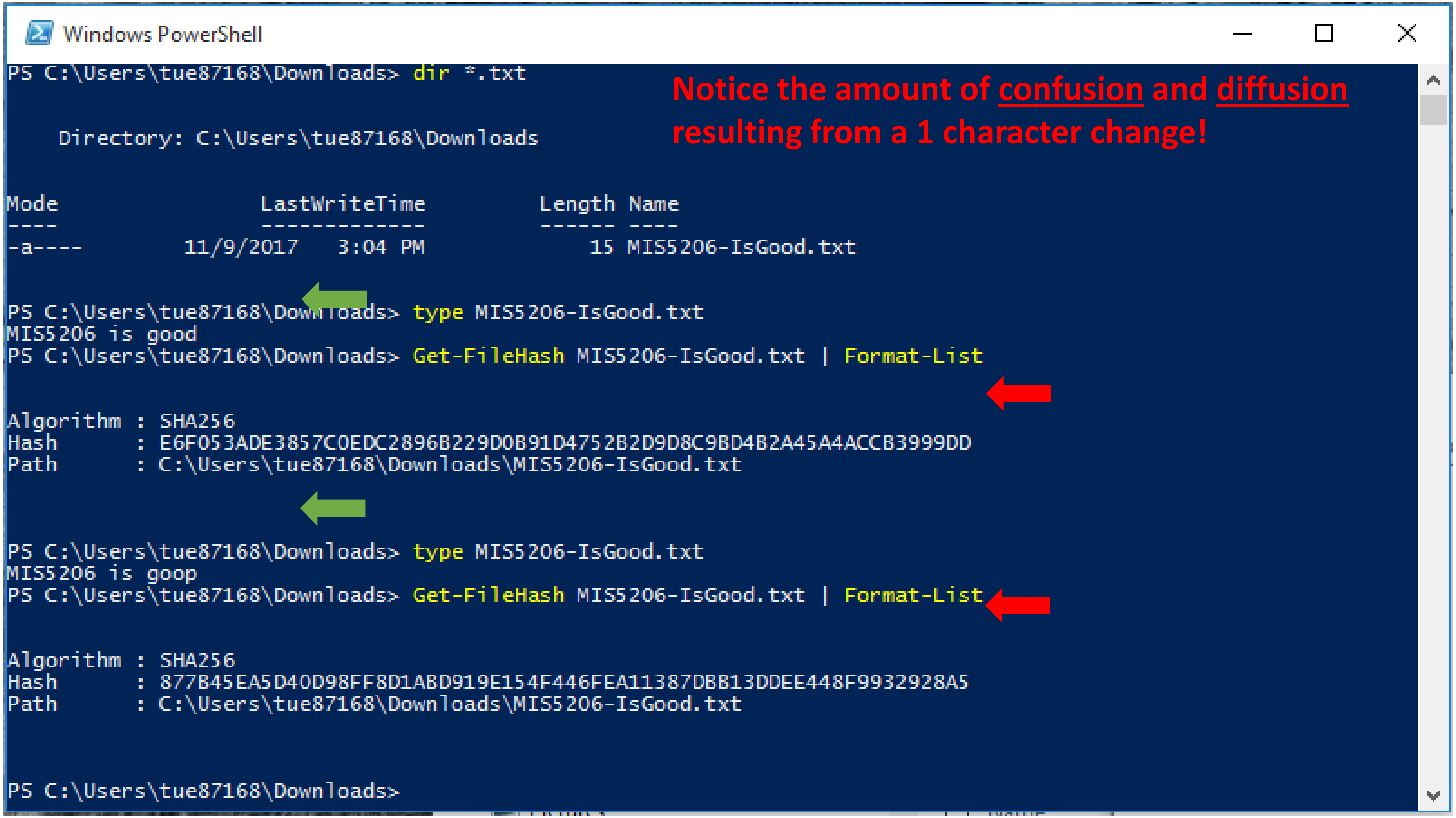


Image Name	Download	Size	Version	sha256sum
Kali 64 bit	HTTP | Torrent	2.8G	2017.2	4556775bfb981ae64a3cb19aa0b73e8dcac6e4ba524f31c4bc14c9137b99725d



```
PS C:\Users\tue87168> cd Downloads
PS C:\Users\tue87168\Downloads> dir *.iso


    Directory: C:\Users\tue87168\Downloads


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        8/10/2017  10:55 AM      674803712 CSET_8.0 (1).iso
-a----        8/10/2017  11:03 AM      674803712 CSET_8.0 (2).iso
-a----        6/12/2017  10:29 AM      674803712 CSET_8.0.iso
-a----        9/27/2017   3:03 PM     2421987328 en_project_professional_2016_x86_x64_dvd_6962236.iso
-a----        10/3/2017   8:49 PM     2421987328 en_visio_professional_2016_x86_x64_dvd_6962139.iso
-a----       11/11/2016  11:45 AM     1469054976 Fedora-Live-Workstation-x86_64-23-10.iso
-a----        11/9/2017   2:31 PM     3020619776 kali-linux-2017.2-amd64.iso


PS C:\Users\tue87168\Downloads> Get-FileHash kali-linux-2017.2-amd64.iso | Format-List


Algorithm : SHA256
Hash      : 4556775BFB981AE64A3CB19AA0B73E8DCAC6E4BA524F31C4BC14C9137B99725D
Path      : C:\Users\tue87168\Downloads\kali-linux-2017.2-amd64.iso



PS C:\Users\tue87168\Downloads> _
```

One-way hash example…

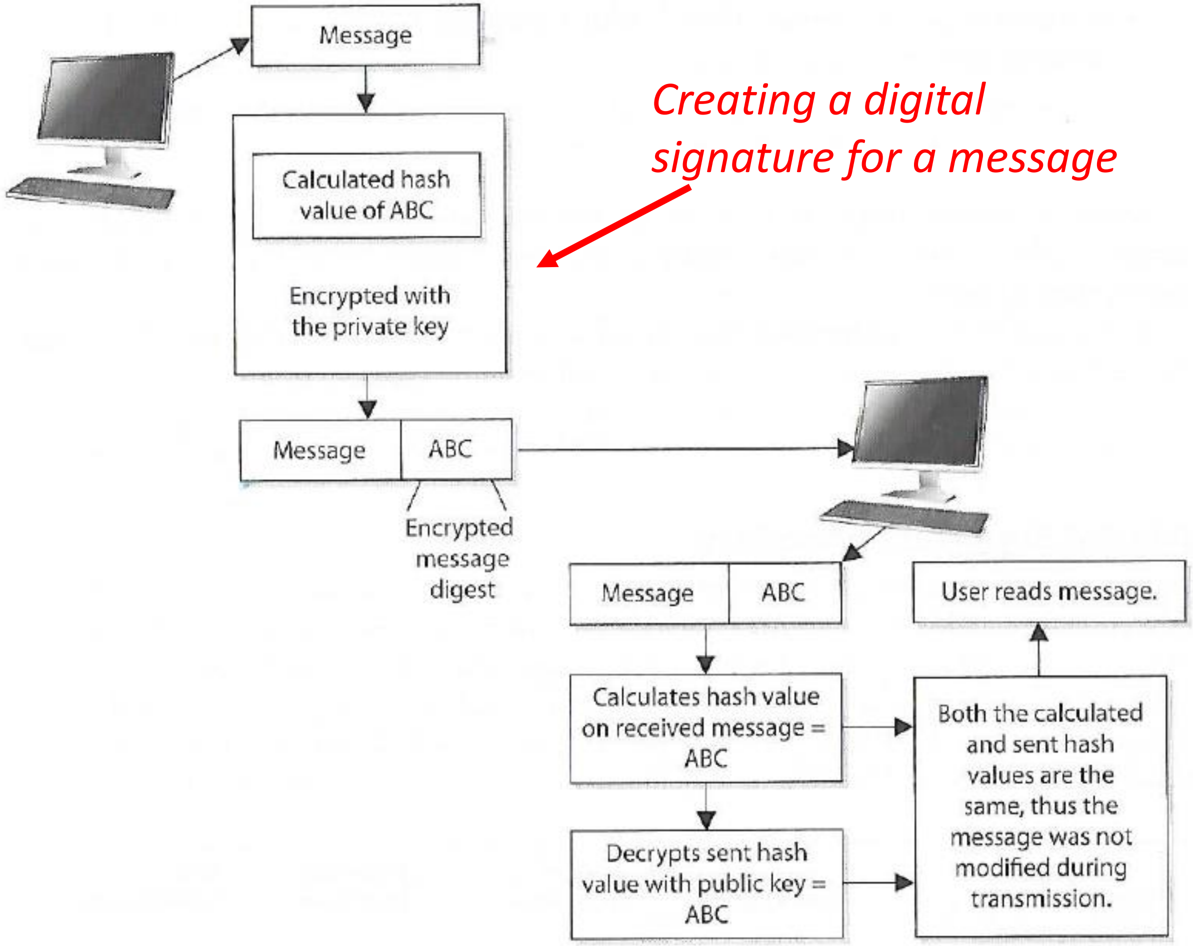


Notice the amount of <u>confusion</u> and <u>diffusion</u> resulting from a 1 character change!

```
PS C:\Users\tue87168\Downloads> dir *.txt


    Directory: C:\Users\tue87168\Downloads


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        11/9/2017   3:04 PM             15 MIS5206-IsGood.txt


PS C:\Users\tue87168\Downloads> type MIS5206-IsGood.txt
MIS5206 is good
PS C:\Users\tue87168\Downloads> Get-FileHash MIS5206-IsGood.txt | Format-List


Algorithm : SHA256
Hash      : E6F053ADE3857C0EDC2896B229D0B91D4752B2D9D8C9BD4B2A45A4ACCB3999DD
Path      : C:\Users\tue87168\Downloads\MIS5206-IsGood.txt



PS C:\Users\tue87168\Downloads> type MIS5206-IsGood.txt
MIS5206 is goop
PS C:\Users\tue87168\Downloads> Get-FileHash MIS5206-IsGood.txt | Format-List


Algorithm : SHA256
Hash      : 877B45EA5D40D98FF8D1ABD919E154F446FEA11387DBB13DDEE448F9932928A5
Path      : C:\Users\tue87168\Downloads\MIS5206-IsGood.txt



PS C:\Users\tue87168\Downloads>
```

Digital Signature

- A hash value encrypted with the sender's private key
- The act of signing means encrypting the message's hash value with the private key



Message
Calculated hash value of ABC
Encrypted with the private key
Message
ABC
Encrypted message digest
Message
ABC
User reads message.
Calculates hash value on received message = ABC
Decrypts sent hash value with public key = ABC
Both the calculated and sent hash values are the same, thus the message was not modified during transmission.

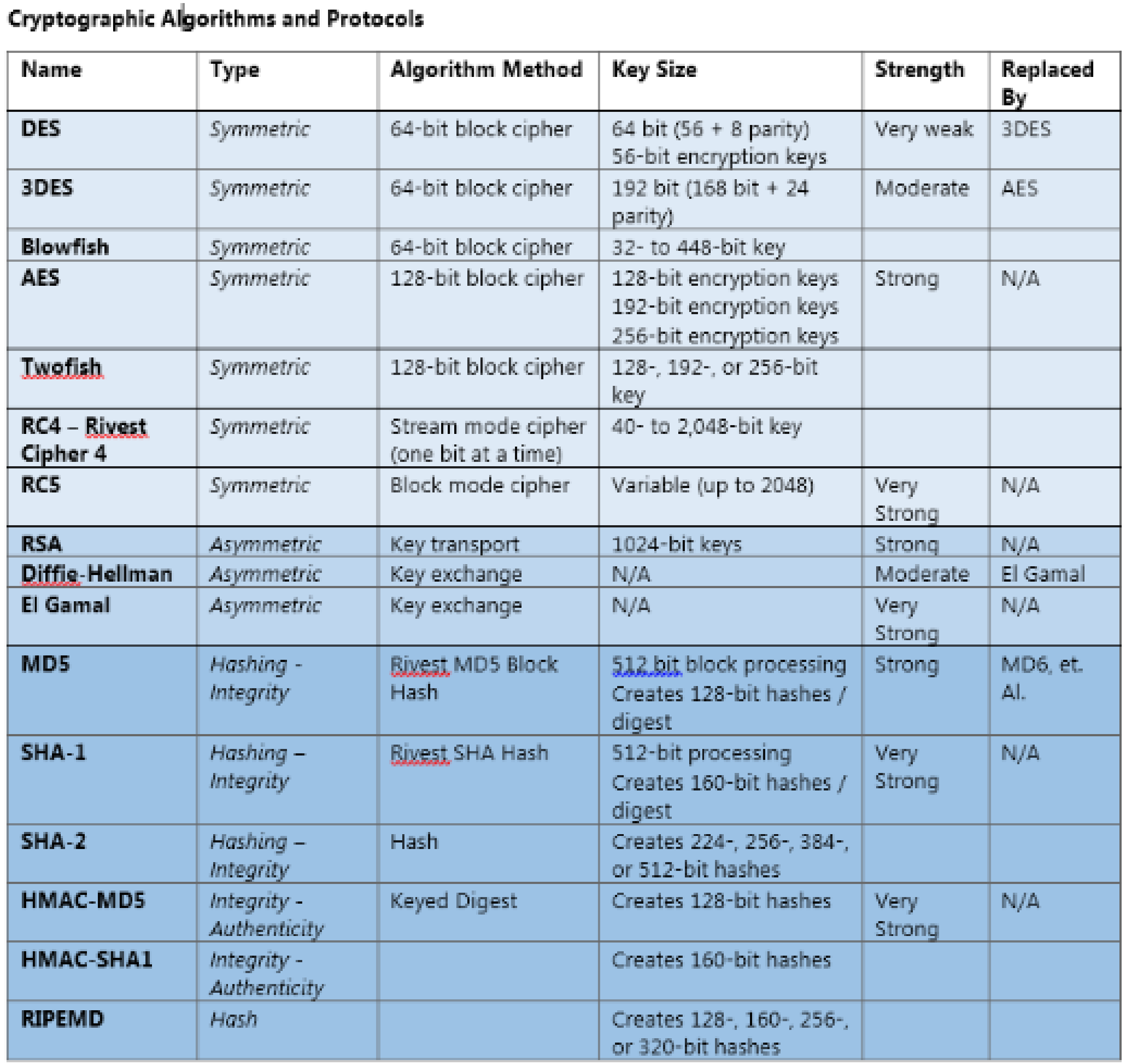
Creating a digital signature for a message

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Message Authentication Codes

- Small block of data generated with a secret key and appended to a message
- HMAC (RFC 2104)
  - Uses hash instead of cipher for speed
  - Used in SSL/TLS and IPSec

Cryptographic algorithms and their functions



Cryptographic Algorithms and Protocols

Name	Type	Algorithm Method	Key Size	Strength	Replaced By
DES	*Symmetric*	64-bit block cipher	64 bit (56 + 8 parity) 56-bit encryption keys	Very weak	3DES
3DES	*Symmetric*	64-bit block cipher	192 bit (168 bit + 24 parity)	Moderate	AES
Blowfish	*Symmetric*	64-bit block cipher	32- to 448-bit key		
AES	*Symmetric*	128-bit block cipher	128-bit encryption keys 192-bit encryption keys 256-bit encryption keys	Strong	N/A
Twofish	*Symmetric*	128-bit block cipher	128-, 192-, or 256-bit key		
RC4 – Rivest Cipher 4	*Symmetric*	Stream mode cipher (one bit at a time)	40- to 2,048-bit key		
RC5	*Symmetric*	Block mode cipher	Variable (up to 2048)	Very Strong	N/A
RSA	*Asymmetric*	Key transport	1024-bit keys	Strong	N/A
Diffie-Hellman	*Asymmetric*	Key exchange	N/A	Moderate	El Gamal
El Gamal	*Asymmetric*	Key exchange	N/A	Very Strong	N/A
MD5	*Hashing - Integrity*	Rivest MD5 Block Hash	512 bit block processing Creates 128-bit hashes / digest	Strong	MD6, et. Al.
SHA-1	*Hashing – Integrity*	Rivest SHA Hash	512-bit processing Creates 160-bit hashes / digest	Very Strong	N/A
SHA-2	*Hashing – Integrity*	Hash	Creates 224-, 256-, 384-, or 512-bit hashes		
HMAC-MD5	*Integrity - Authenticity*	Keyed Digest	Creates 128-bit hashes	Very Strong	N/A
HMAC-SHA1	*Integrity - Authenticity*		Creates 160-bit hashes		
RIPEMD	*Hash*		Creates 128-, 160-, 256-, or 320-bit hashes		

Reasons to Use Cryptography

Reason	How achieved
Confidentiality	The message can be encrypted
Integrity	The message can be hashed and/or digitally signed
Authentication	The message can be digitally signed
Nonrepudiation	The message can be digitally signed

Public Key Infrastructure

- Not the same as public key encryption algorithm
- All components needed to enable secure communication
  - Policies and Procedures
  - Keys and Algorithms
  - Software and Data Formats
- Assures identity to users
- Provides key management features

PKI Components

Digital Certificates

- Contains Public Key identity and verification info

Certificate Authorities (CA)

- Trusted entity that issues certificates

Registration Authorities (RA)

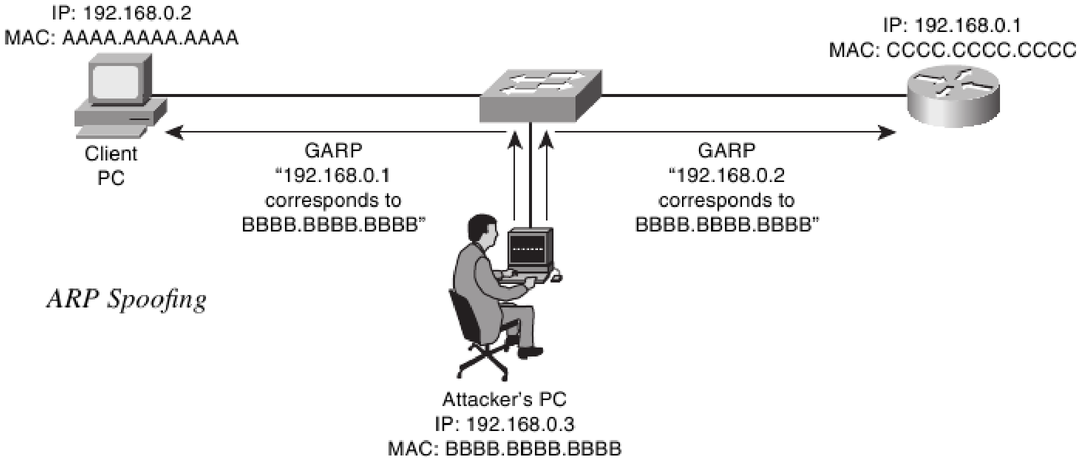
- Verifies identity for certificate requests

Certificate Revocation List (CRL)

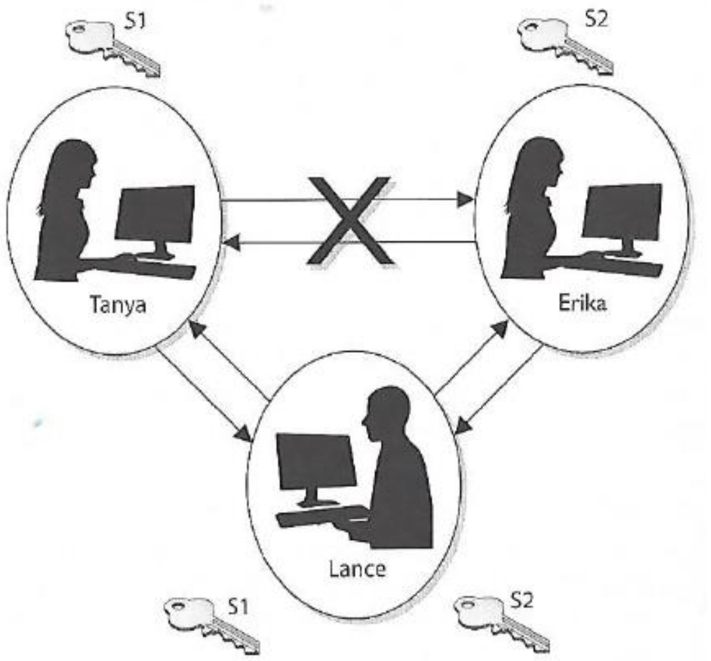
Cryptanalysis Attacks

Man-in-the-Middle attack

- Hacker intercepts traffic grabs two others’ public keys and replaces them with his/her own public key and uses his/her own private key to decrypt and monitors the traffic between the others



ARP Spoofing



Cryptanalysis Attacks

- Brute force
  - Trying all key values in the keyspace
- Frequency Analysis
  - Guess values based on frequency of occurrence
- Dictionary Attack
  - Find plaintext based on common words
- Replay Attack
  - Repeating previous known values
- Factoring Attacks
  - Find keys through prime factorization
- Known Plaintext
  - Format or content of plaintext available

Cryptanalysis Attacks

- Chosen Plaintext
  - Attack can encrypt chosen plaintext
- Chosen Ciphertext
  - Decrypt known ciphertext to discover key
- Differential Power Analysis
  - Side Channel Attack
  - Identify algorithm and key length