Protecting Information Assets
- Unit# 11 -

Cryptography, Public Key Encryption and Digital Signatures

Agenda

- Cryptography and Cryptanalysis
- Terminology
- Symmetric Cryptography
- Asymmetric Cryptography
- Hashing and Digital Signature
- Public Key Infrastructure
- Cryptanalysis Attacks
- Quiz

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

The etymology is Greek and means: “*secret writing*”

Where do you look for encryption related controls?

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

Control Enhancements:

(1) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

(2) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*

The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST FIPS-compliant; NSA-approved*] key management technology and processes.

(3) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].

(4) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*

[Withdrawn: Incorporated into SC-12].

(5) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*

[Withdrawn: Incorporated into SC-12].

References: NIST Special Publications 800-56, 800-57.

Priority and Baseline Allocation:

P1	**LOW** SC-12	**MOD** SC-12	**HIGH** SC-12 (1)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39

SC-13 CRYPTOGRAPHIC PROTECTION

Control: The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements: None.

(1) *CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(2) *CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(3) *CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*
[Withdrawn: Incorporated into SC-13].

(4) *CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.

Priority and Baseline Allocation:

P1	LOW SC-13	MOD SC-13	HIGH SC-13

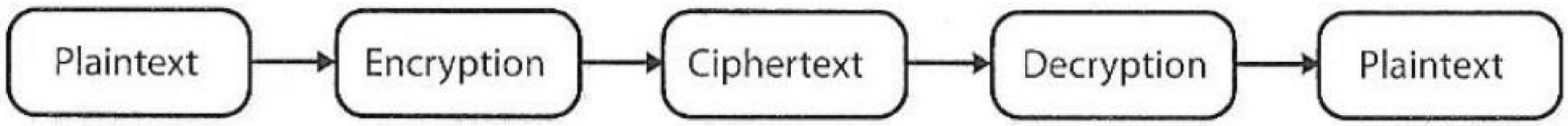
Cryptanalysis

- 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

Services of cryptosystems

- **Confidentiality** – Renders 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, requested or provided the information
  - ***Authorization*** *– On proving identity, the individual is provided with the key or password that will permit access to some resource*
- **Nonrepudiation** – Ensure the sender cannot deny sending the information

Repudiation – the sender denying he sent the message

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

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

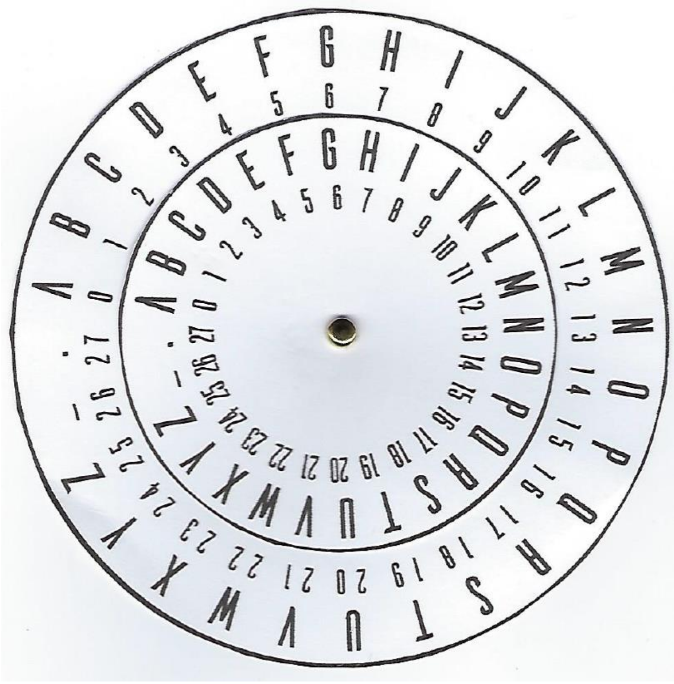
- **Plaintext:**
  LOGICAL SECURITY
- **Ciphertext:**
  ORJLFDO VHFXULWB

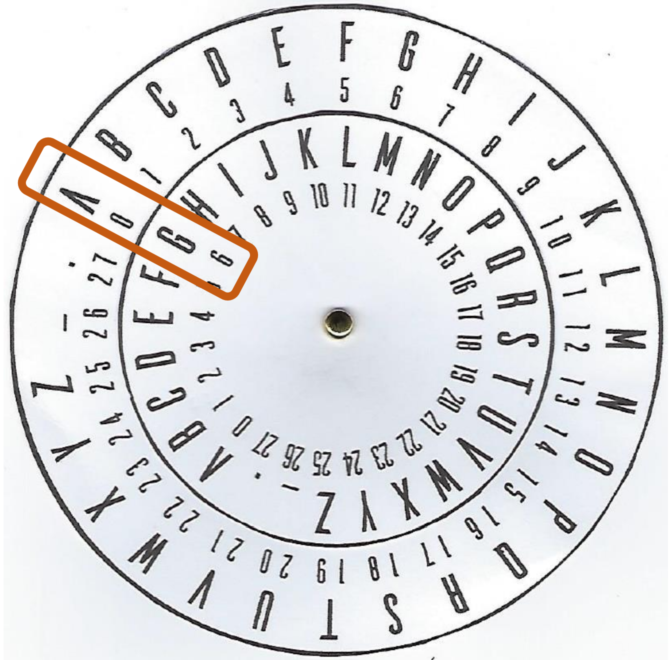
Cipher Disk

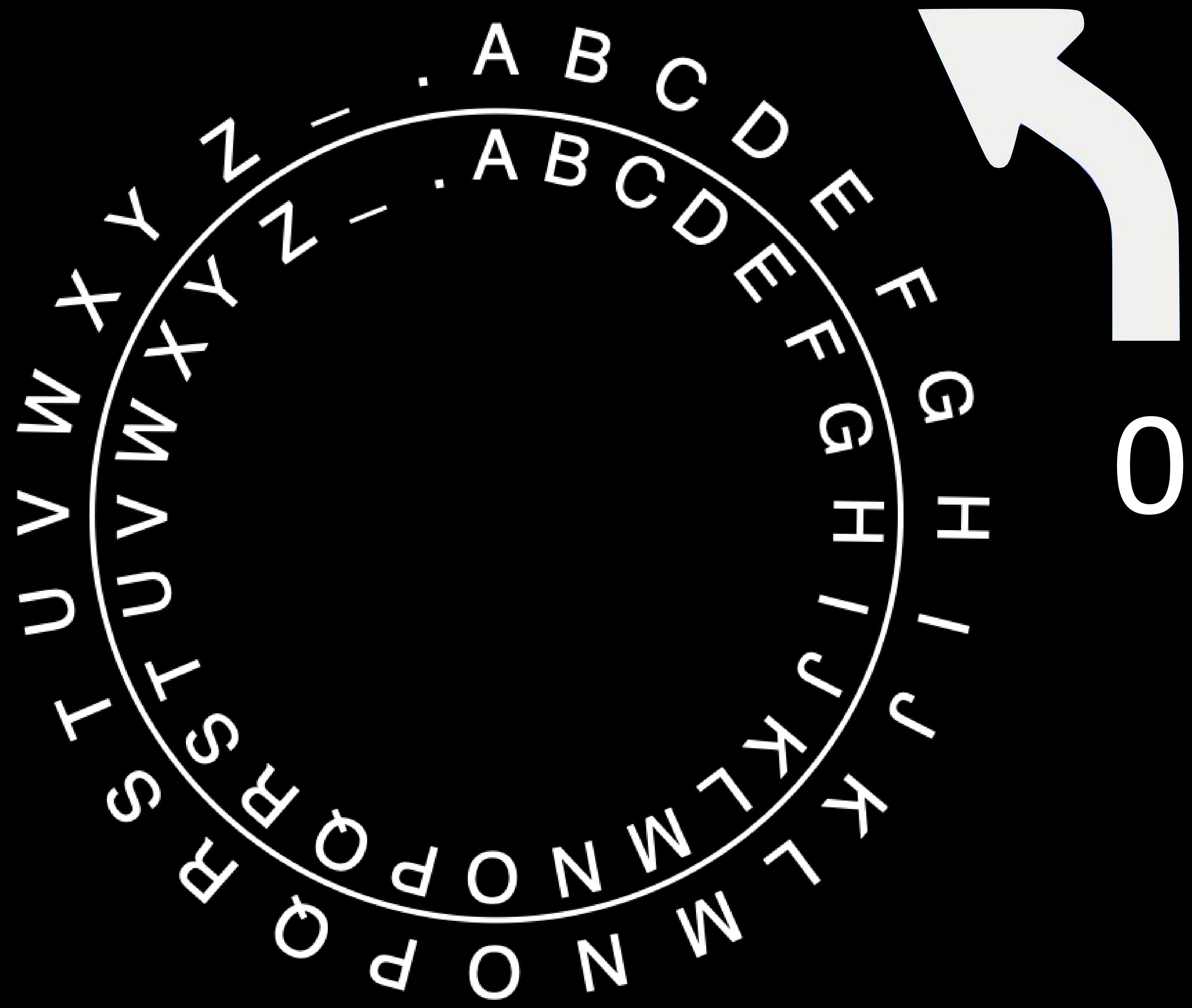
Outer wheel is for the *plaintext* alphabet

Inner wheel is for *ciphertext*

When the outer wheel and inner wheel and are both aligned at the letter “A” (i.e. position zero), there is no encryption mapping the letters on the outer wheel to letters on the inner wheel

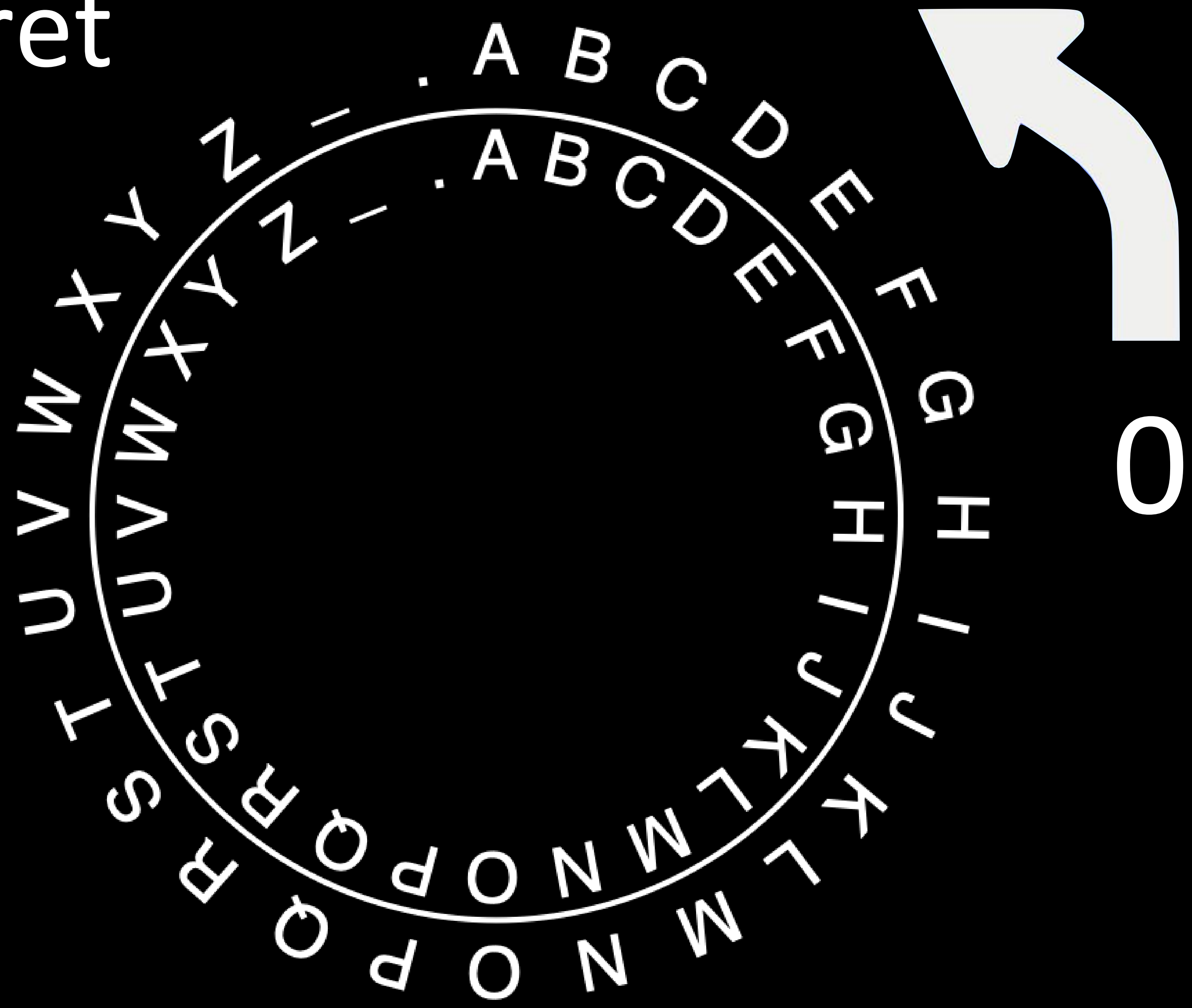




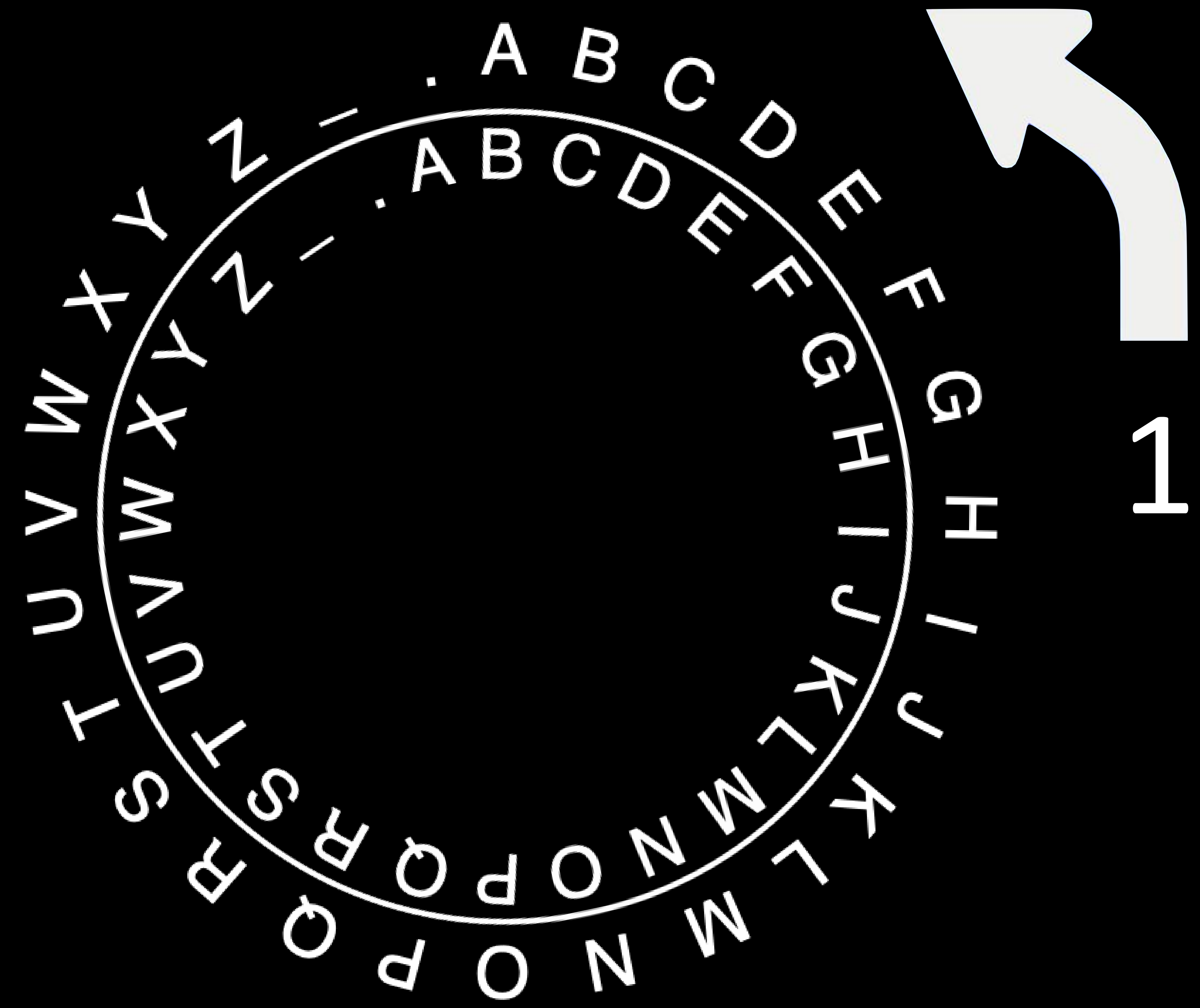


. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
0

Secret

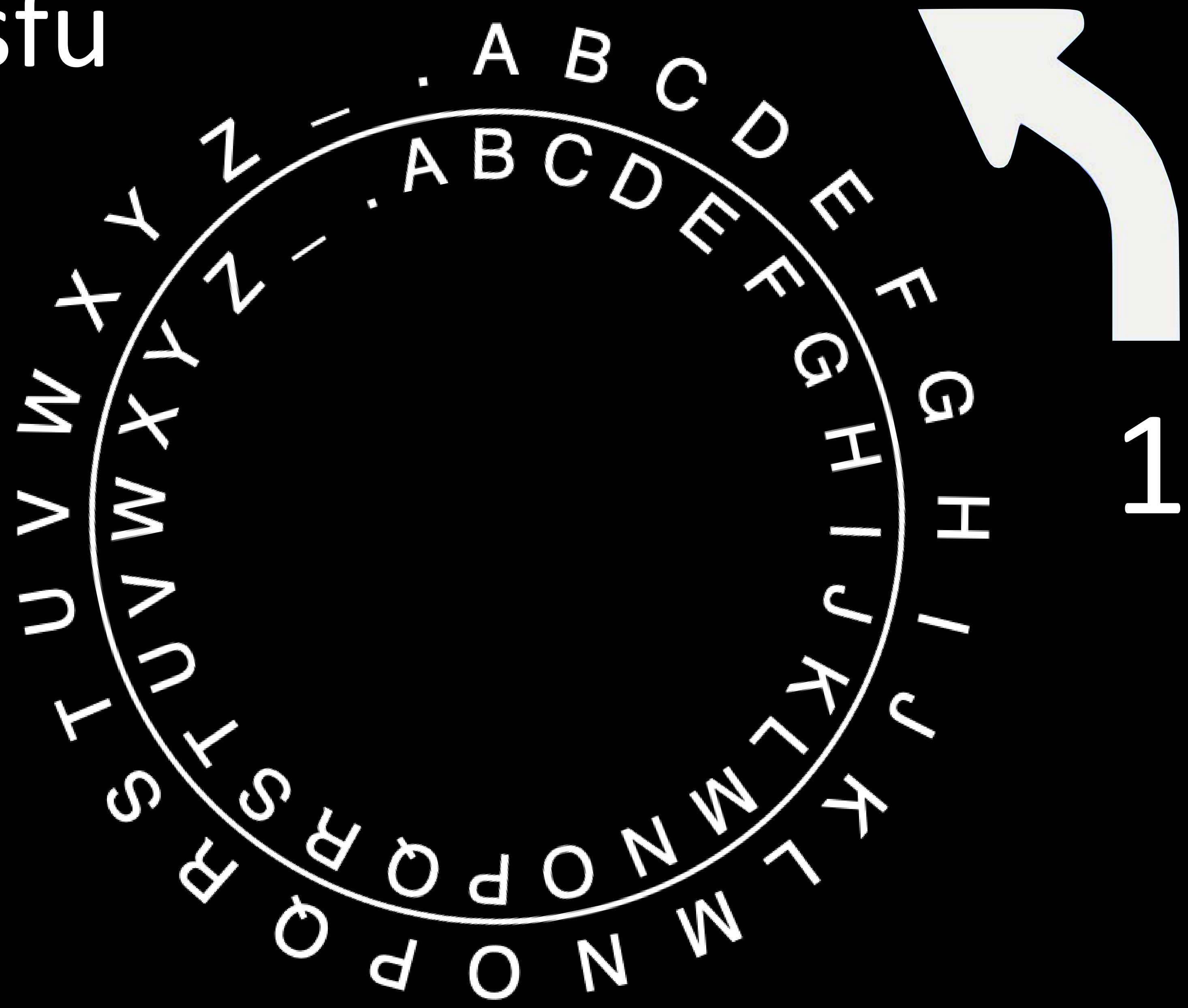


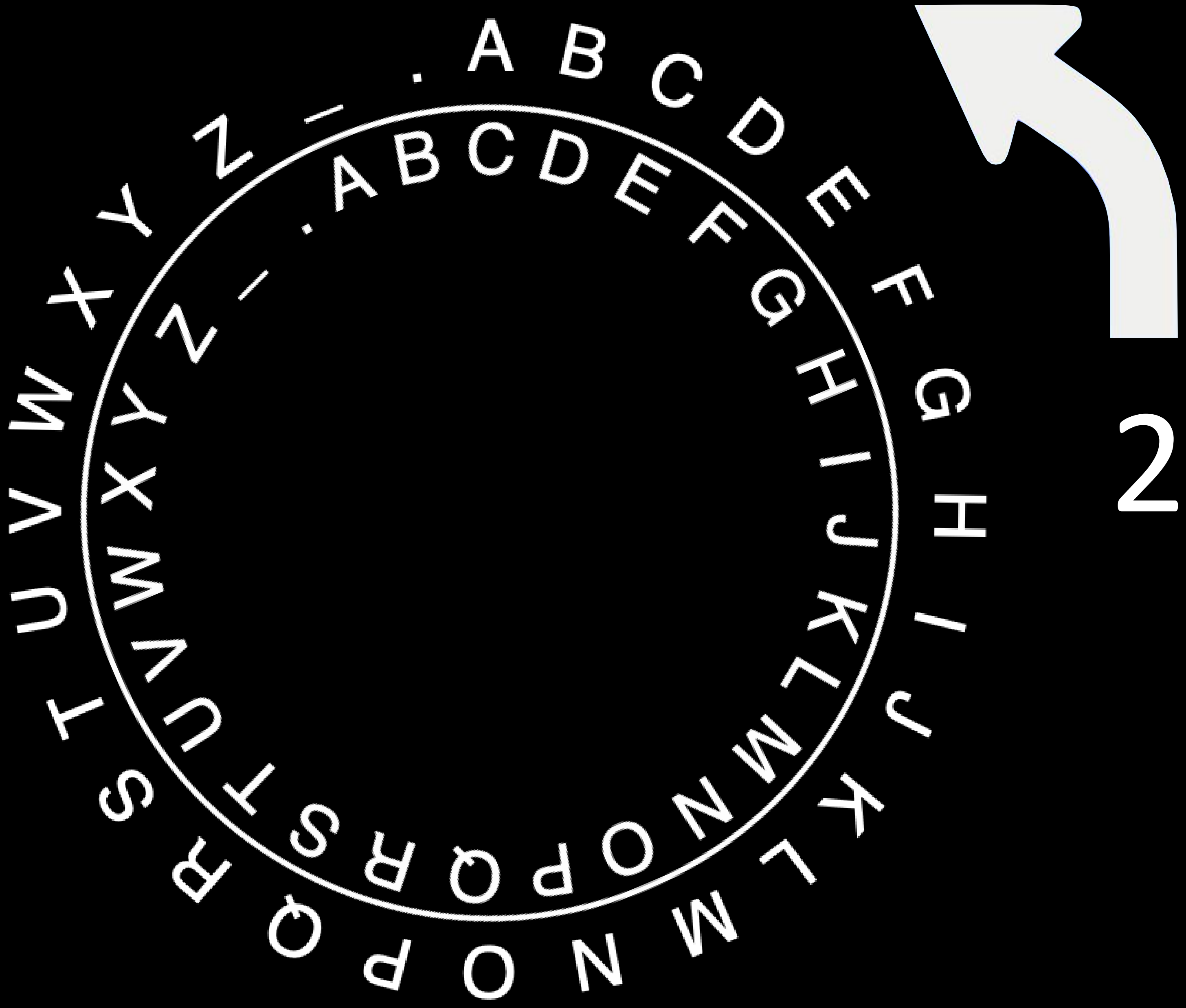
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
0



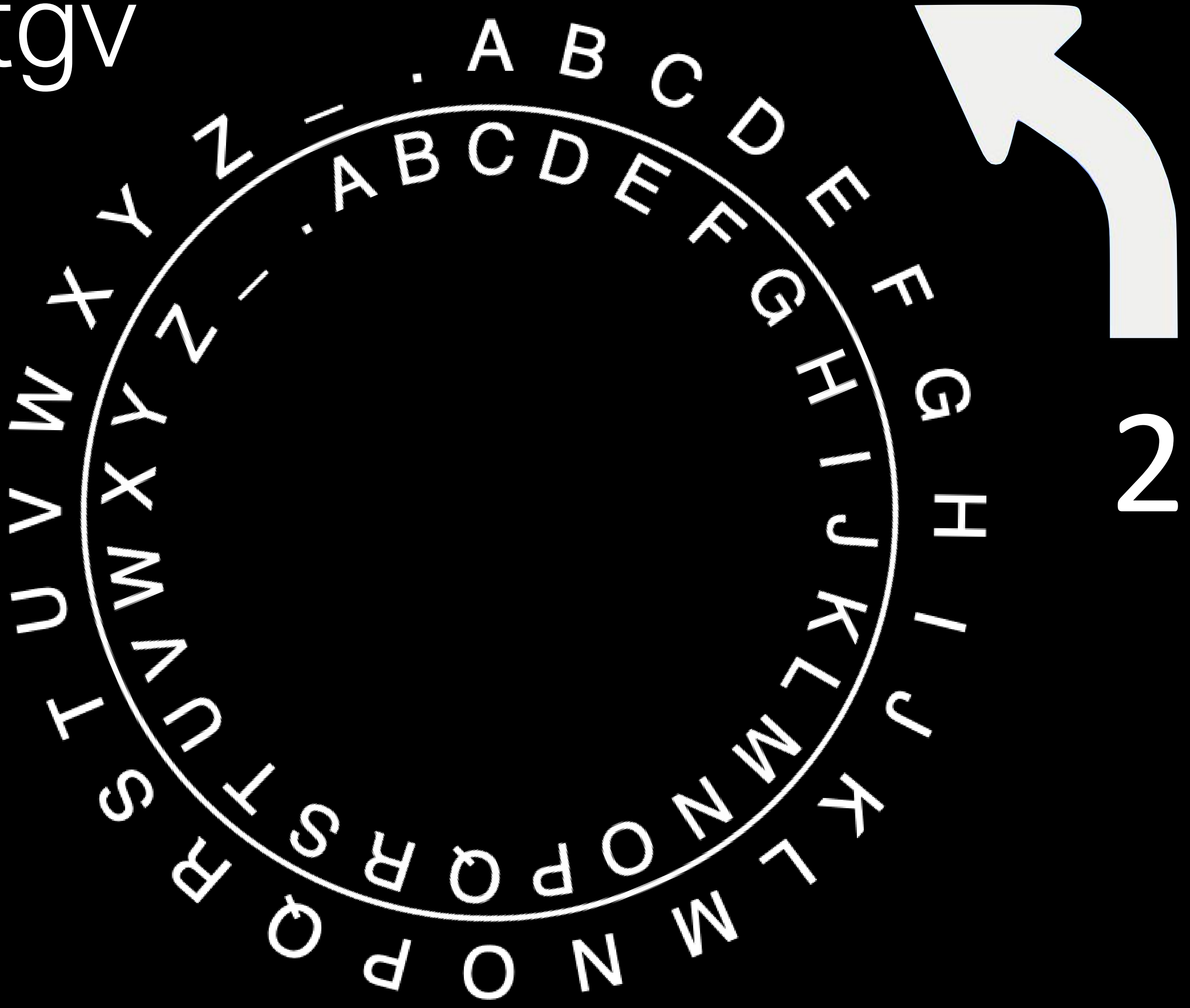
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
1

Tfdsfu


. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
1

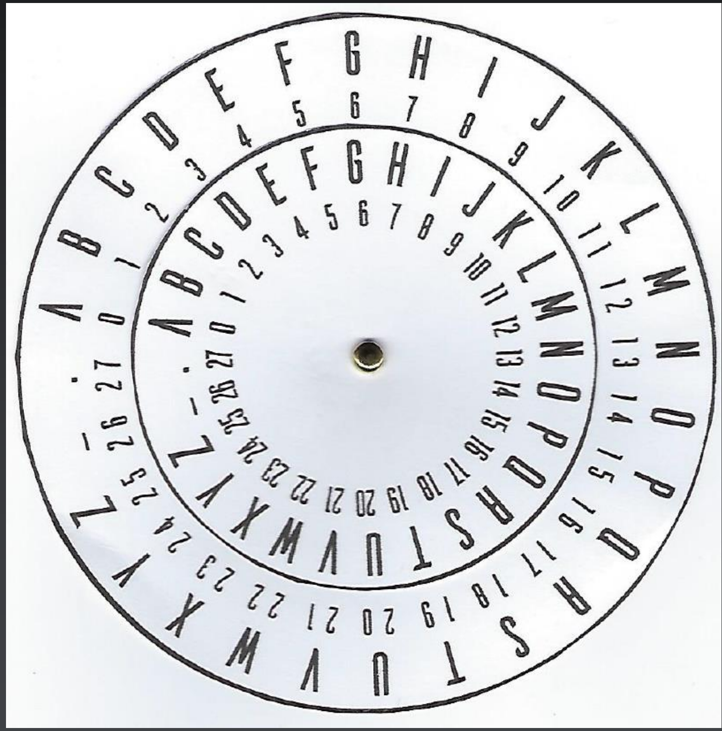

. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
2

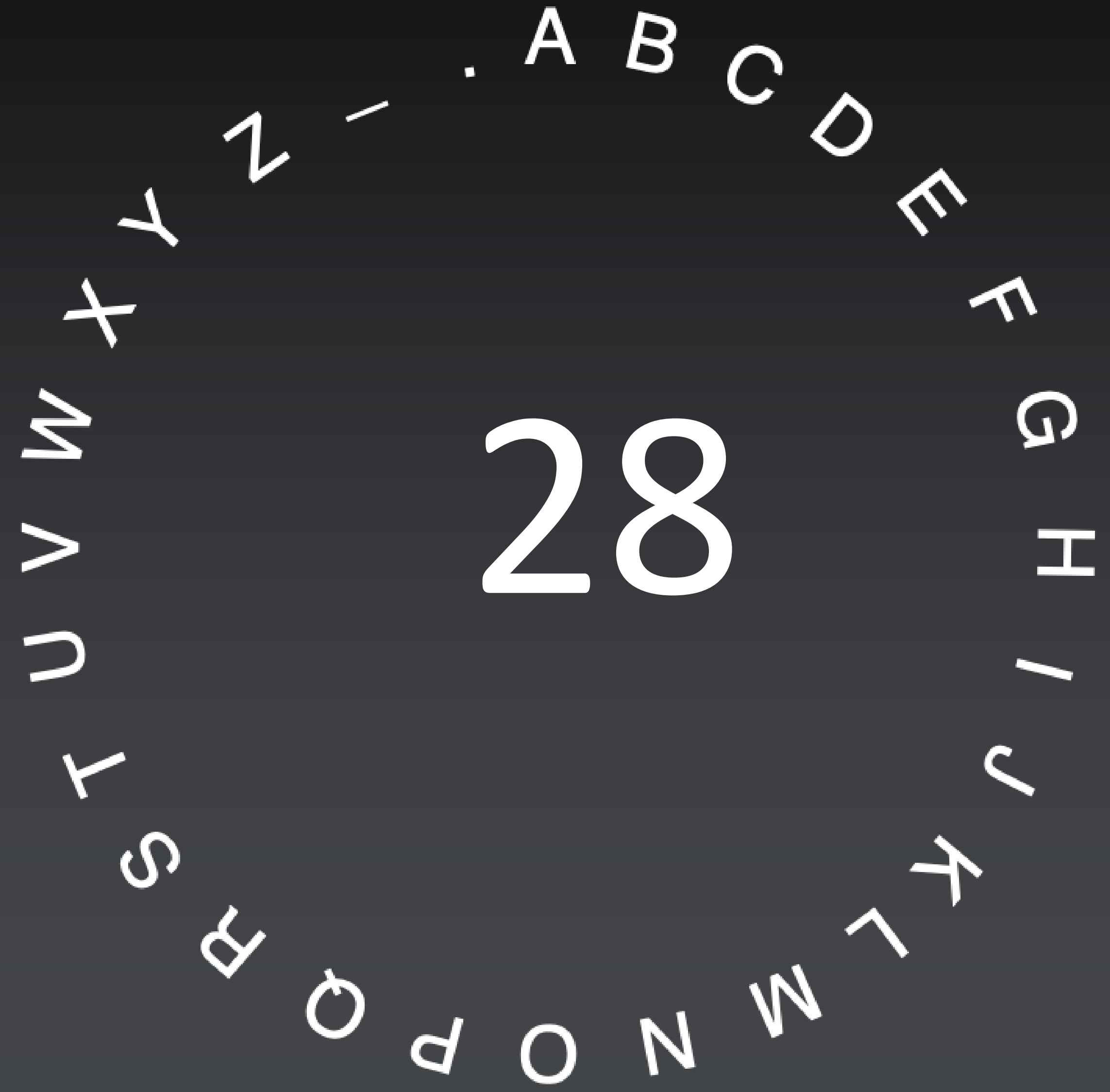
Ugetgv



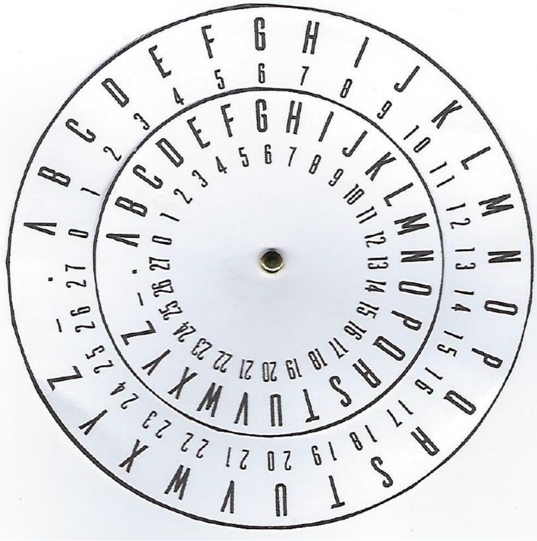
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _
2

Keyspace is the number of possible keys



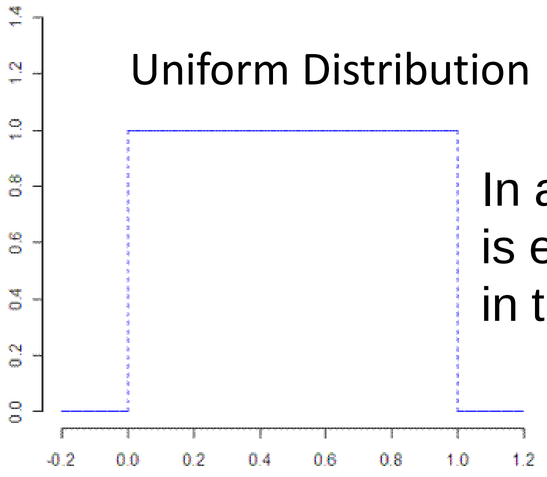


Question B: Assuming each key is equally likely (randomly distributed) how many random guesses would you have to make on average to find the key to decrypt the plaintext?



- Answer: ~14, (28 -1) = 27 and 27/2 = 13.5 which is approximately 14
  - Because the <u>average</u> of a uniform distribution is half
  - Recall 26 letters in the alphabet + "." and "-" = 28, but we cannot use "0" as the key which gives us the original plaintext back the size of the alphabet

Uniform Distribution



In a uniform distribution any number is equally likely, the average is right in the middle, or half the distribution

- This is important in cryptography because <u>on average</u> the number of attempts needed to successfully guess the key through brute forcing is half of the key space
- This is true of the simple cipher wheel as well as modern encryption schemes with very large key spaces

Linguistic cryptanalysis examples…

- Recognizing the beginning of the word
- Looking for letter pairs
- Looking at vowels

This form of cryptanalysis uses your knowledge of the English language

Linguistic cryptanalysis examples…

One form of linguistic cryptanalysis is *frequency analysis of letters used in English*

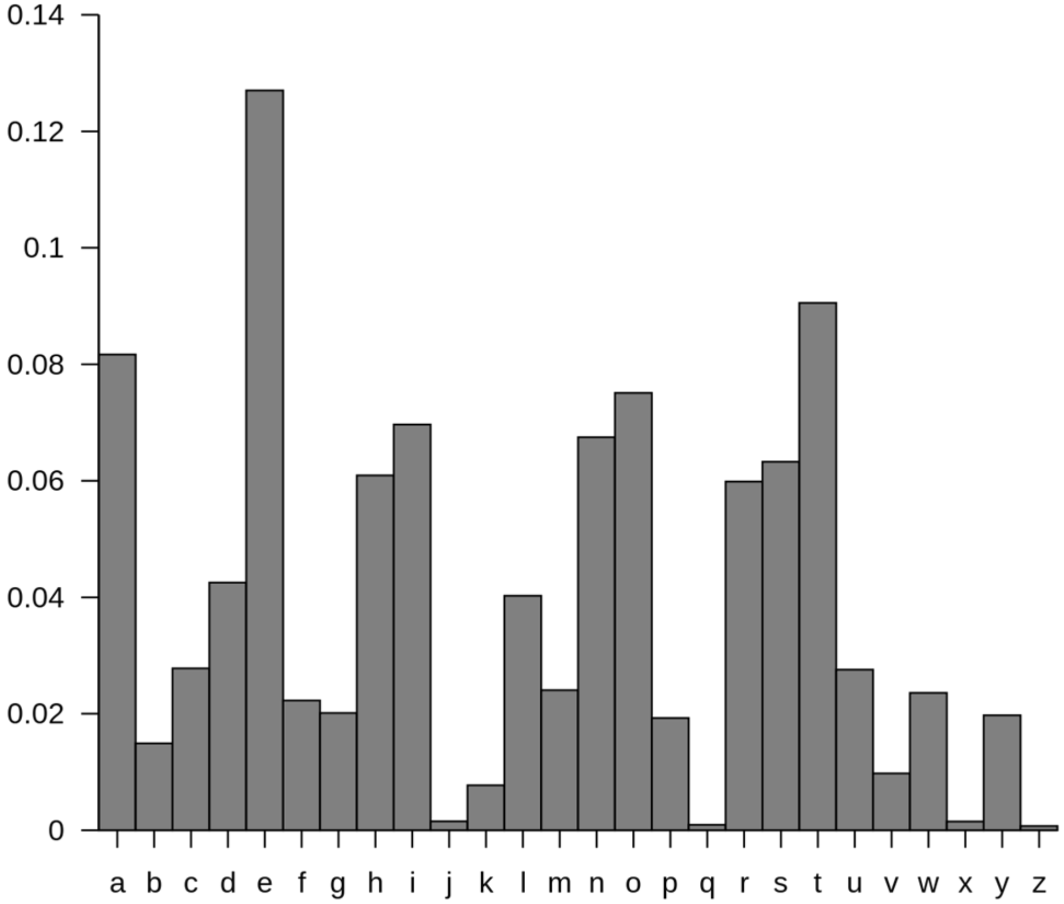
Frequency analysis recognizes that different letters have different probabilities of frequencies of use in words:

Given a sentences written in the English language

- E, T, A and O are the most common
- Z, Q and X are rare

- TH, ER, ON, and AN are the most common pairs of letters (termed bigrams or digraphs)

- SS, EE, TT, and FF are the most common repeats



Example: Substitution cipher or algorithm

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

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

Polyalphabetic Cipher

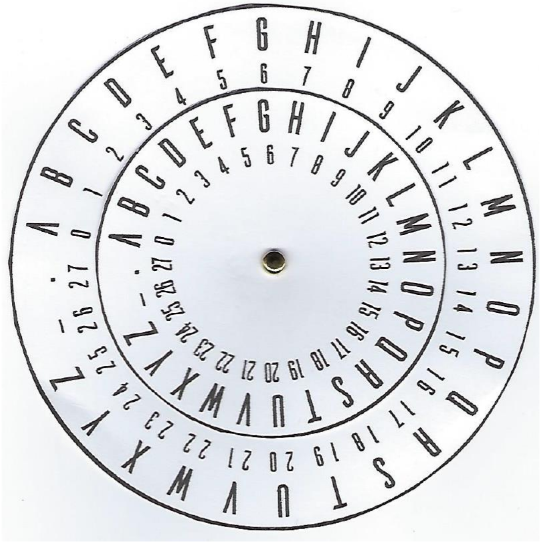
Ciphers can be made stronger, and frequency analysis made more difficult when more than one cipher alphabet is used

- For example, encrypt the plaintext message "SEND MONEY"
  - Use the word "SECURITY" as the key, but repeat its use in the key to make it have as many letters as the plaintext:

Plaintext: SEND MONEY (10 characters including the space "_")

Key: SECURITYSE (10 characters)

1. Encrypt by rotating the inner wheel so that "s" in the word "security" aligns with "a" on the outer wheel. Now "s" in the word "send" on the outer wheel maps to the letter "i" on the inner wheel, so "i" is the ciphertext.



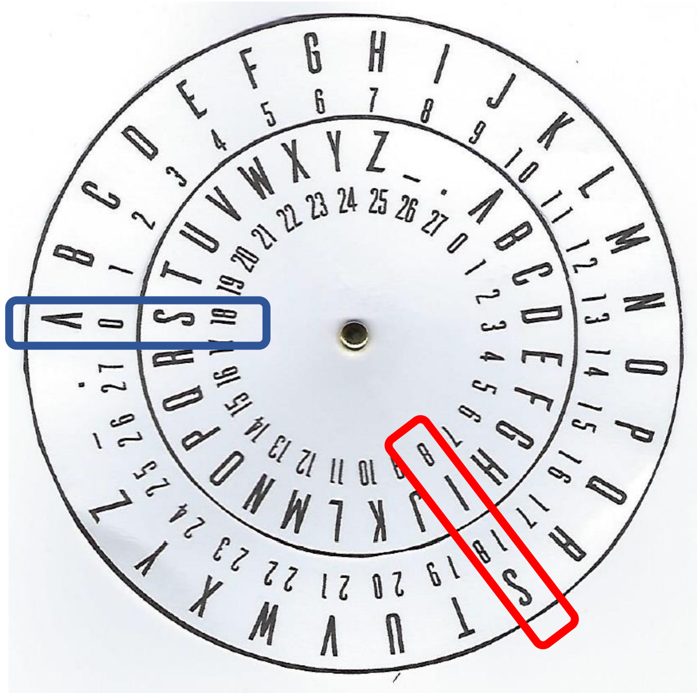
Polyalphabetic Cipher

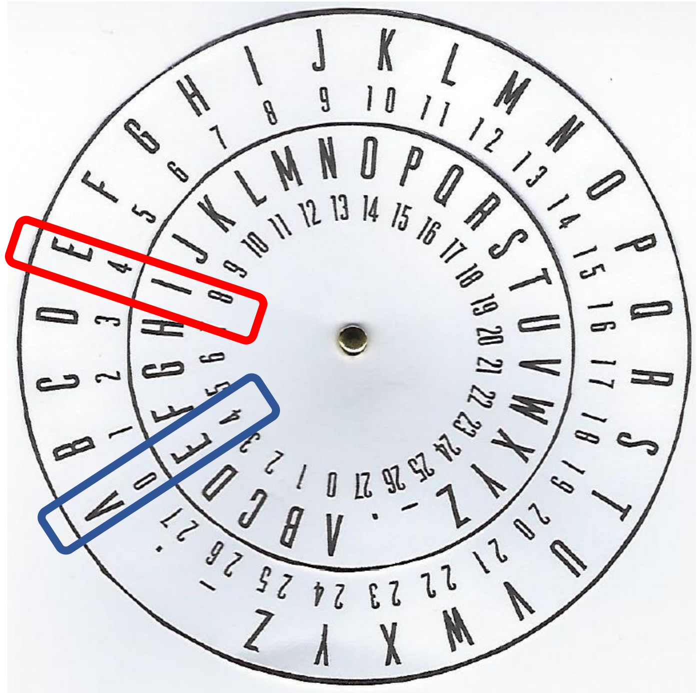
Plaintext: SEND MONEY (10 characters including the space "_")

Key: SECURITYSE (10 characters)

1. Encrypt by rotating the inner wheel so that "S" in the word "SECURITY" aligns with "A" on the outer wheel
   Now "S" in the word "SEND" on the outer wheel maps to the letter "I" on the inner wheel, so "I" is the ciphertext

2. Next, rotate the inner wheel so that "E" in the word "SECURITY" aligns with "A" on the outer wheel. Now "E" in the word "SEND" on the outer wheel maps to "I" on the inner wheel, so "I" is the ciphertext again, even though the plaintext is different than before





Question: What is the rest of the ciphertext for "SEND MONEY" using the polyalphabetic key "SECURITY"?

IIPXPUFJWA

Polyalphabetic ciphers make frequency analysis more difficult

Polyalphabetic substitution is another building block of cryptography

Random Polyalphabetic Cipher

What if we use a random polyalphabetic key that is as long as the message?

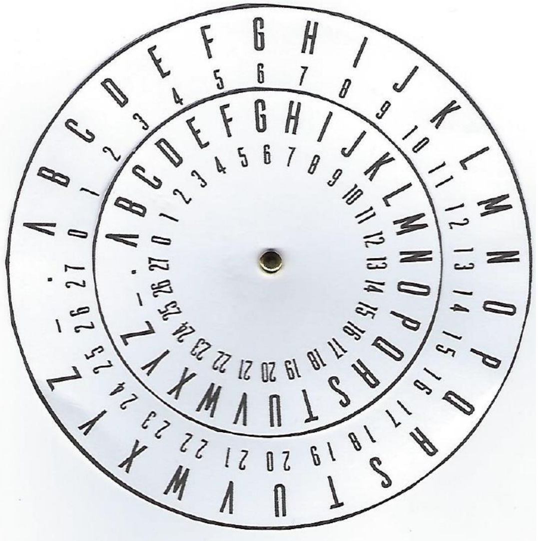
For example, let's say our plaintext is:

We intend to begin on the first of February unrestricted submarine warfare.

And the polyalphabetic key is a string of random characters as long as the message:

ackwulsjwkblogbzcukn.kqubpnnefjvcebuymaclzvzmzwfbxpmmzqwmm.tejzf

Question: How would an attacker could attempt to crack this message?
Is an attack possible?



Cipher = encryption algorithm

2 main attributes combined in a cypher

1. **Confusion:** usually carried out through substitution
   - *Let’s look at another way to do substitution*

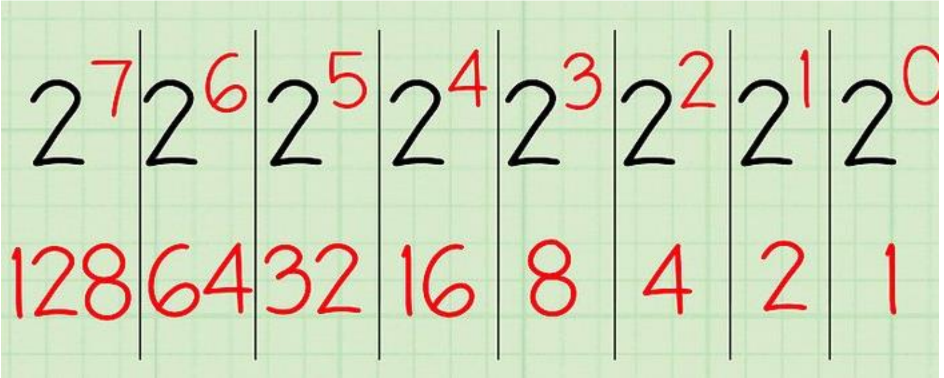
2. **Diffusion:** Usually carried out through transposition

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

Binary – Decimal

Decimal - ASCII

0	0	0	0	0	0	0	0	=	0
1	1	1	1	1	1	1	1	=	255



Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e

ASCII Character Table

Name	Hex	Dec
. (period)	2E	046
0	30	048
1	31	049
2	32	050
3	33	051
4	34	052
5	35	053
6	36	054
7	37	055
8	38	056
9	39	057

Name	Hex	Dec
A	41	065
B	42	066
C	43	067
D	44	068
E	45	069
F	46	070
G	47	071
H	48	072
I	49	073
J	4A	074
K	4B	075

Name	Hex	Dec
L	4C	076
M	4D	077
N	4E	078
O	4F	079
P	50	080
Q	51	081
R	52	802
S	53	083
T	54	084
U	55	085
V	56	086

Name	Hex	Dec
W	57	087
X	58	088
Y	59	089
Z	5A	090

8 bits supports 256 numbers

XOR – Exclusive OR

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

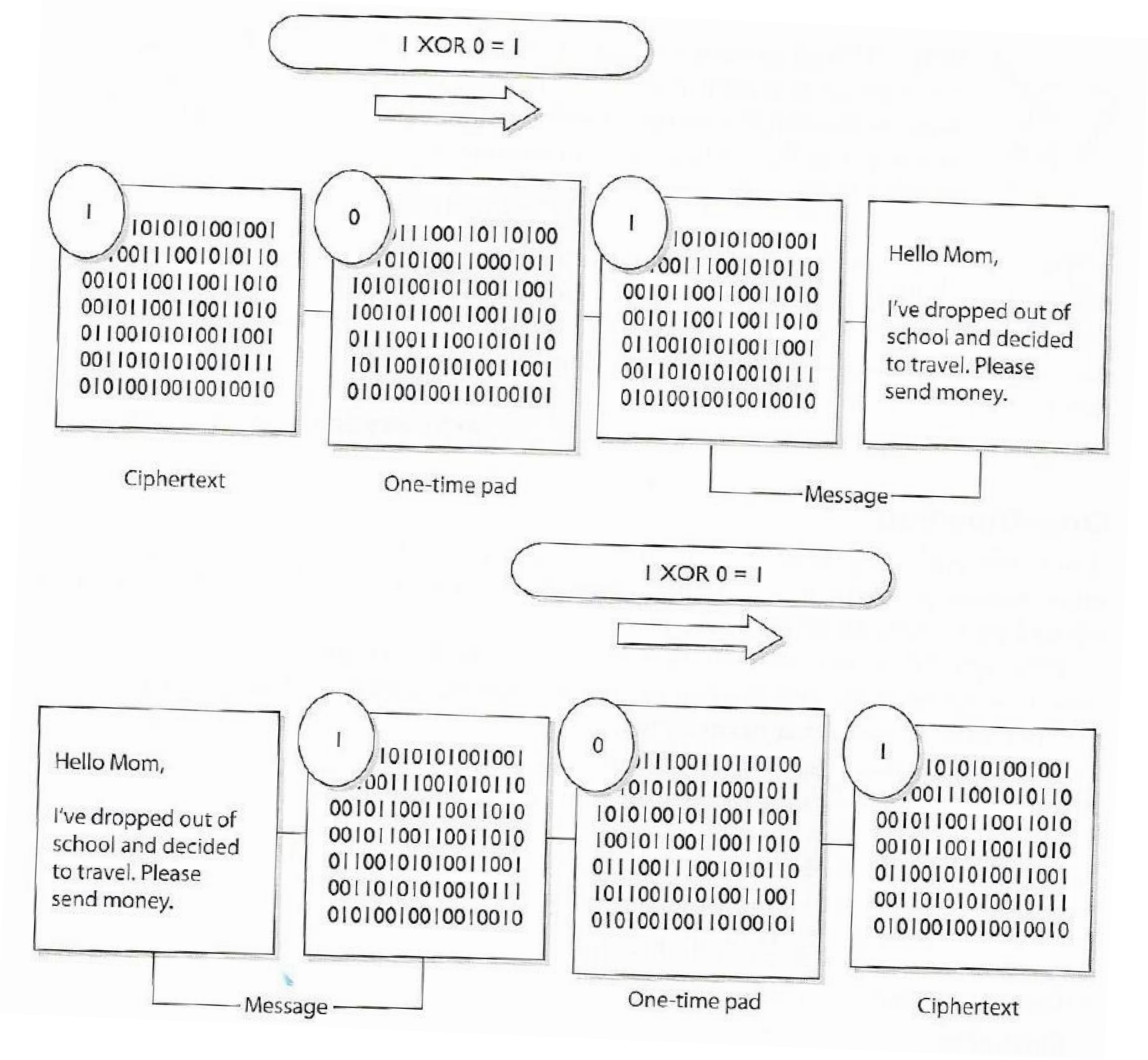
Message stream:	1001010111
Keystream:	0011101010
Ciphertext stream:	1010111101

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

One-Time Pad *a perfect encryption scheme*

One-Time Pad Requirements

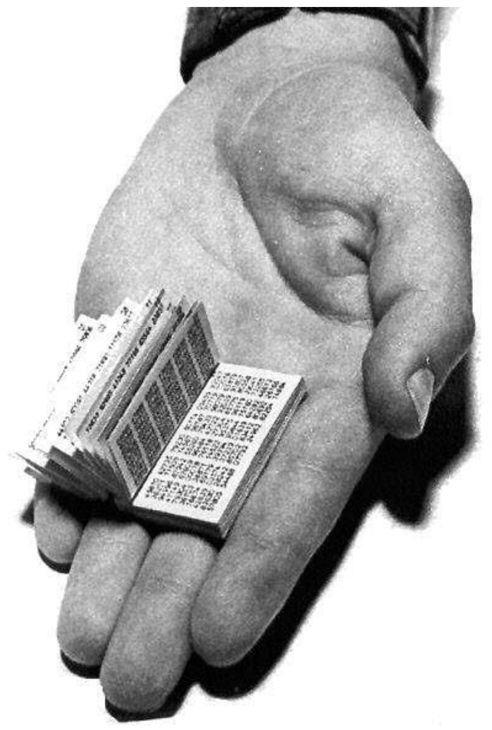
- Made up of truly random values
- Used only one time
- Securely distributed to its destination
- Secured at sender's and receiver's sites
- At least as long as the message



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

One-time pad -- Problems

- Must be *perfectly random*
- Pad must be as long as the message
- Must be used **only once**
    - Skimp on any of these conditions, it becomes trivial to break your system
- Any software product claiming to use one-time pad is **snake-oil**.
    - Computers are bad at generating *truly* random numbers



Cipher = encryption algorithm

2 main attributes combined in a cypher

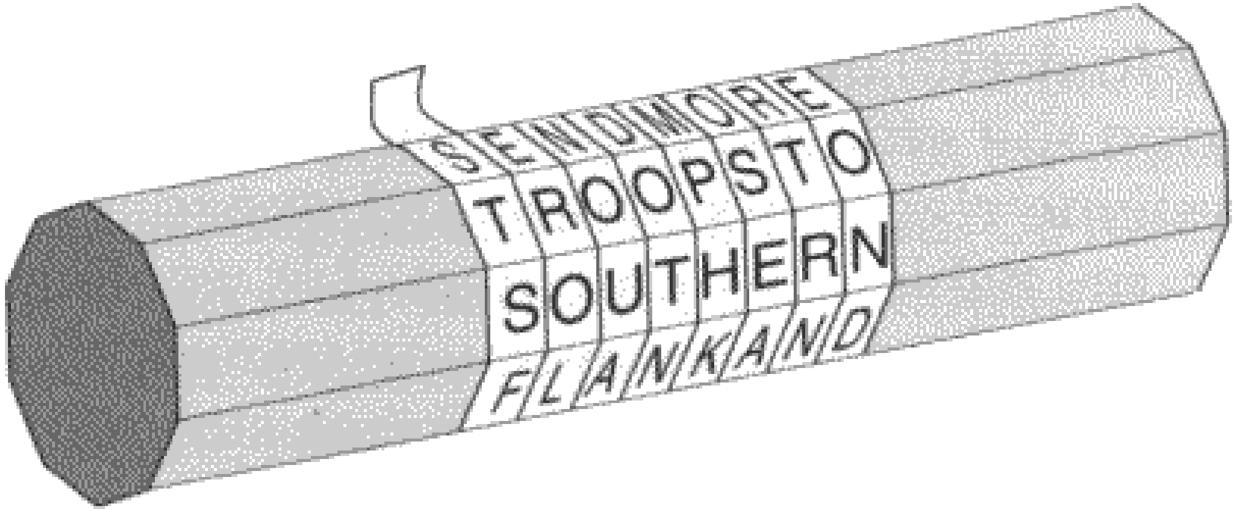
1. **Confusion:** usually carried out through substitution

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

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

Transposition

- Ancient example: scytale



A profit was achieved by our ACT unit

a pr o f i t wa s
a c hi e v e d b y
o u r a c t u ni t

0 1 2 3 4 5 6 7 8 9

a p r o f i t w a s

a c h i e v e d b y

o u r a c t u n i t

6	0	2	5	4	8	7	1	3	9
t	a	r	i	f	a	w	p	o	s
e	a	h	v	e	b	d	c	i	y
u	o	r	t	c	i	n	u	a	t

0 1 2 3 4 5 6 7 8 9

a p r o f i t w a s

a c h i e v e d b y

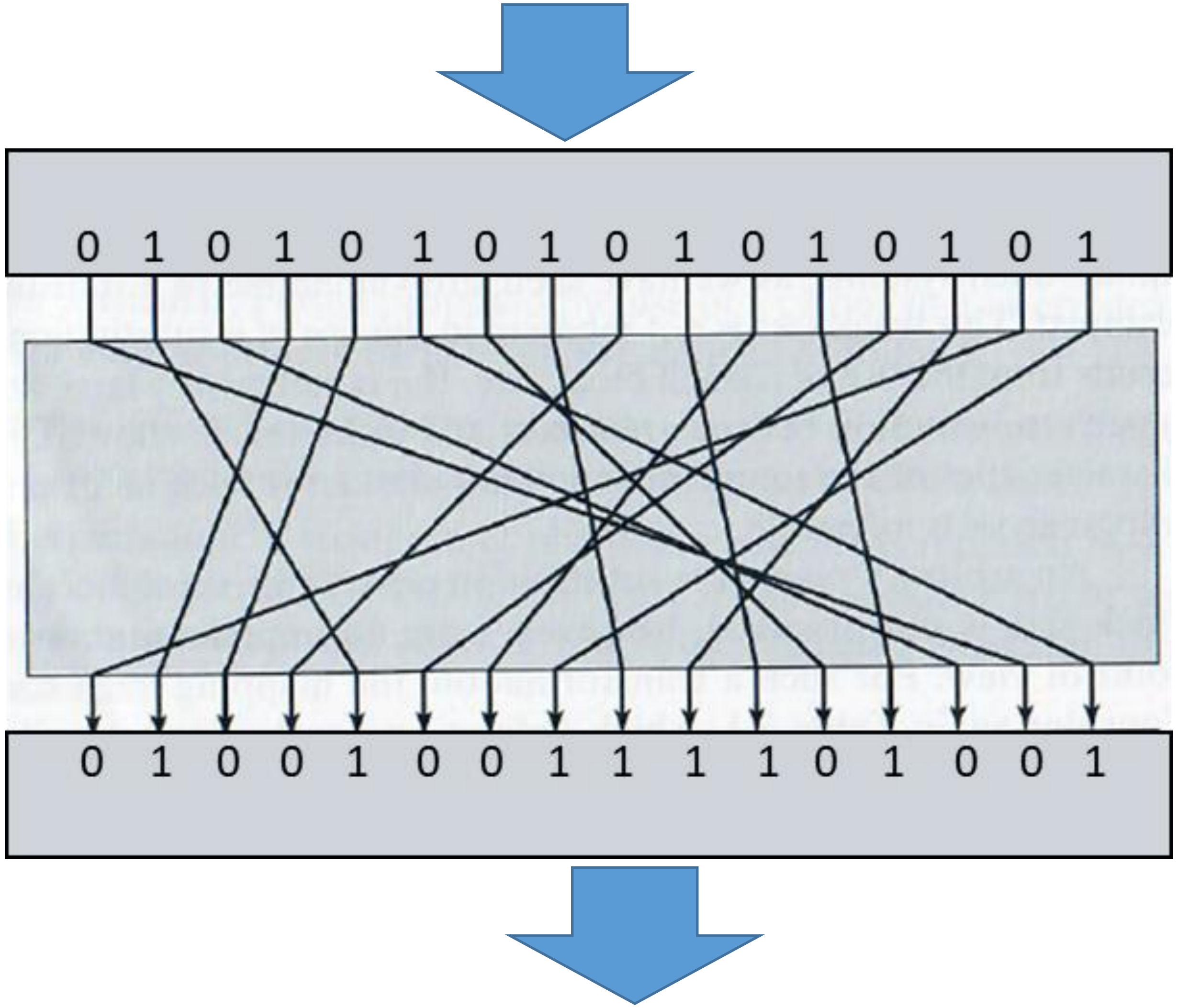
o u r a c t u n i t

2 main attributes combined in a cypher

1. Confusion: usually carried out through substitution

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

0101010101010101



0100100111101001

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

Examples of dichotomies in cryptography

- Symmetric versus Asymmetric
- Stream versus block
- 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.

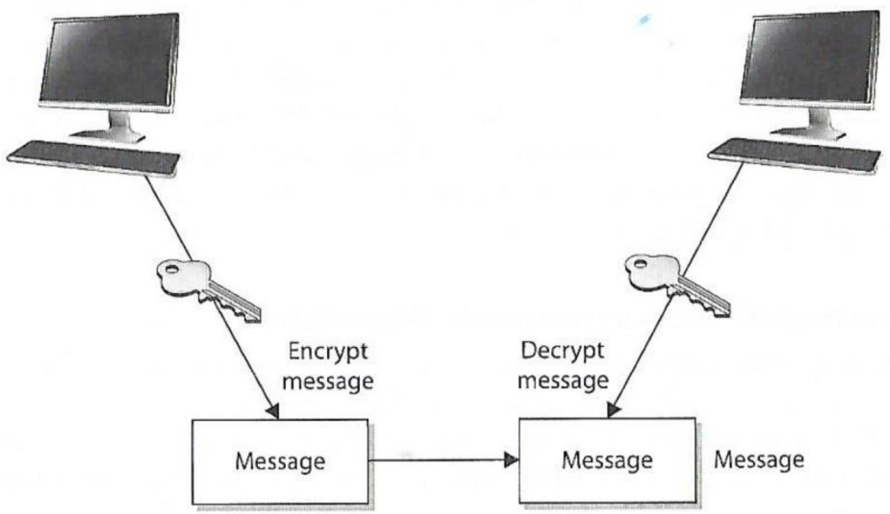
Weaknesses:

- 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.

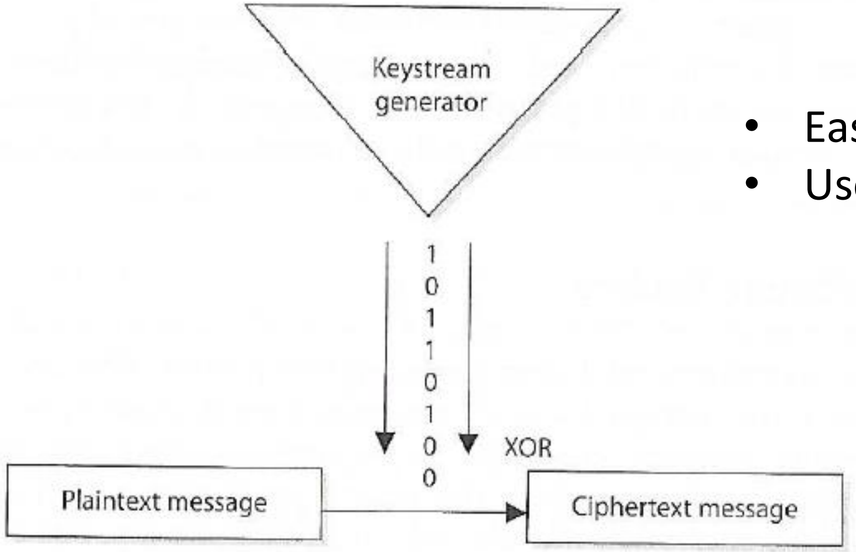
Two types: Stream and Block Ciphers

- **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

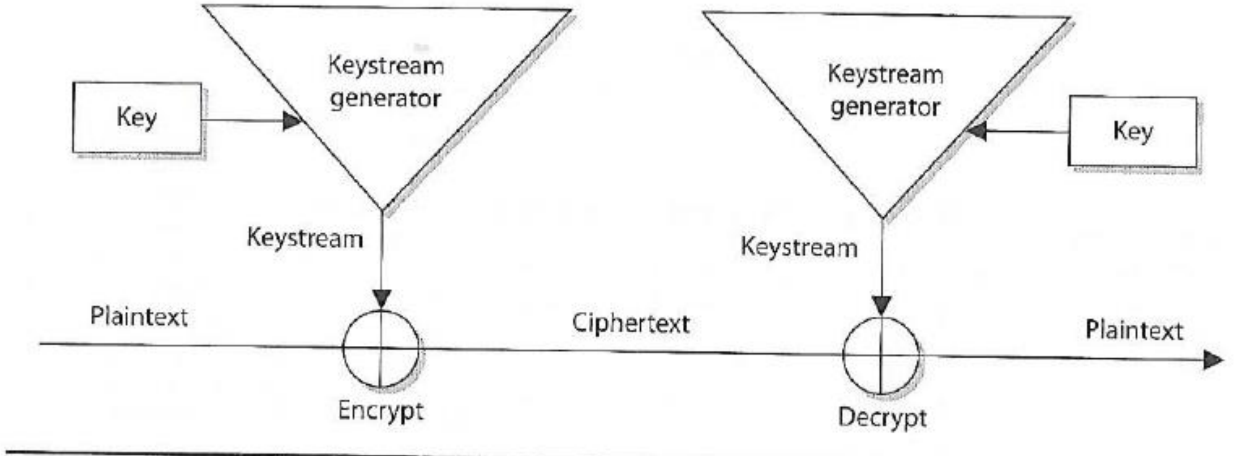
Symmetric encryption uses the same keys.



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) <u>All-In-One CISSP Exam Guide</u>, McGraw Hill Education

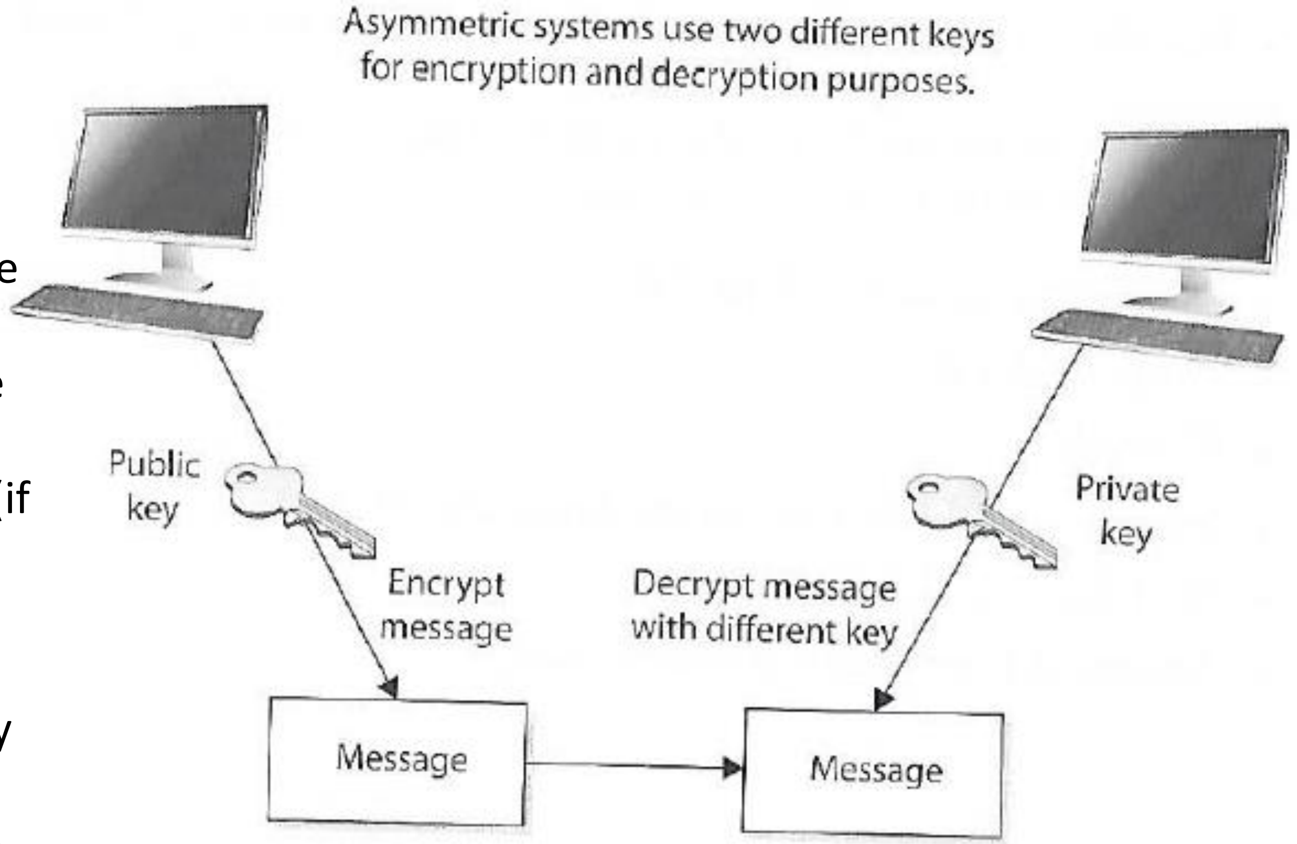
Symmetric versus asymmetric algorithms

- 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 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

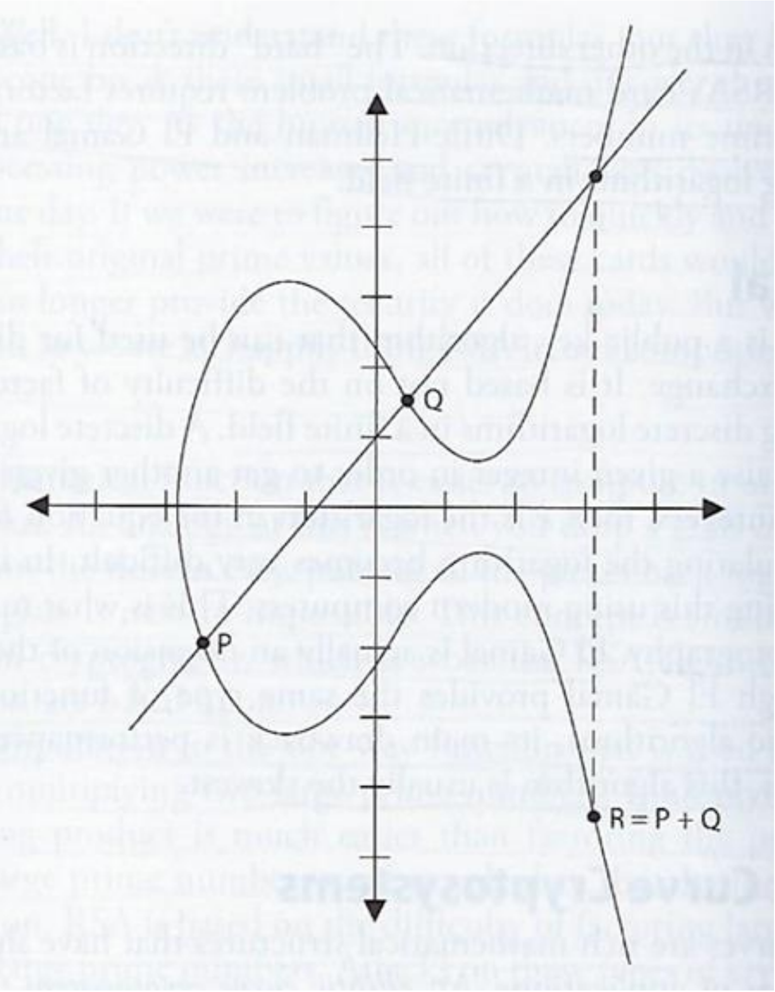
- If **confidentiality** is the most important security service, the sender would encrypt the file with the receiver’s public key
  - This is called a “**secure message format**” because it can only be decrypted by the person with the corresponding private key

- 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
  - <u>Confidentiality is not assured</u>

Cryptographic algorithms and their functions

Elliptical curve cryptography (ECC) is a public key encryption technique (Asymmetric)

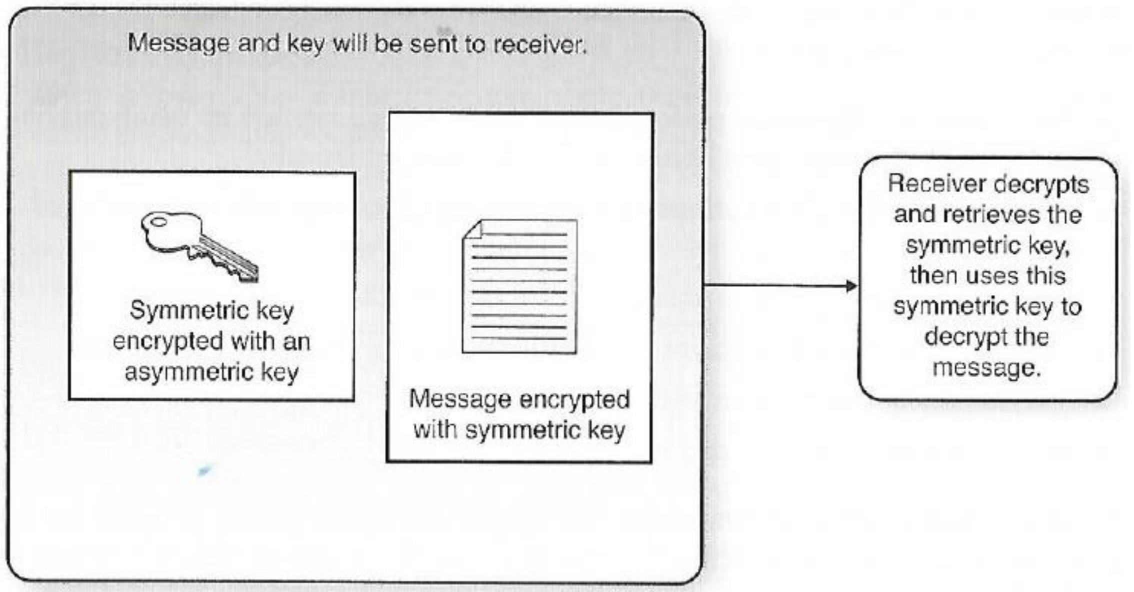
- Based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys
- ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers



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

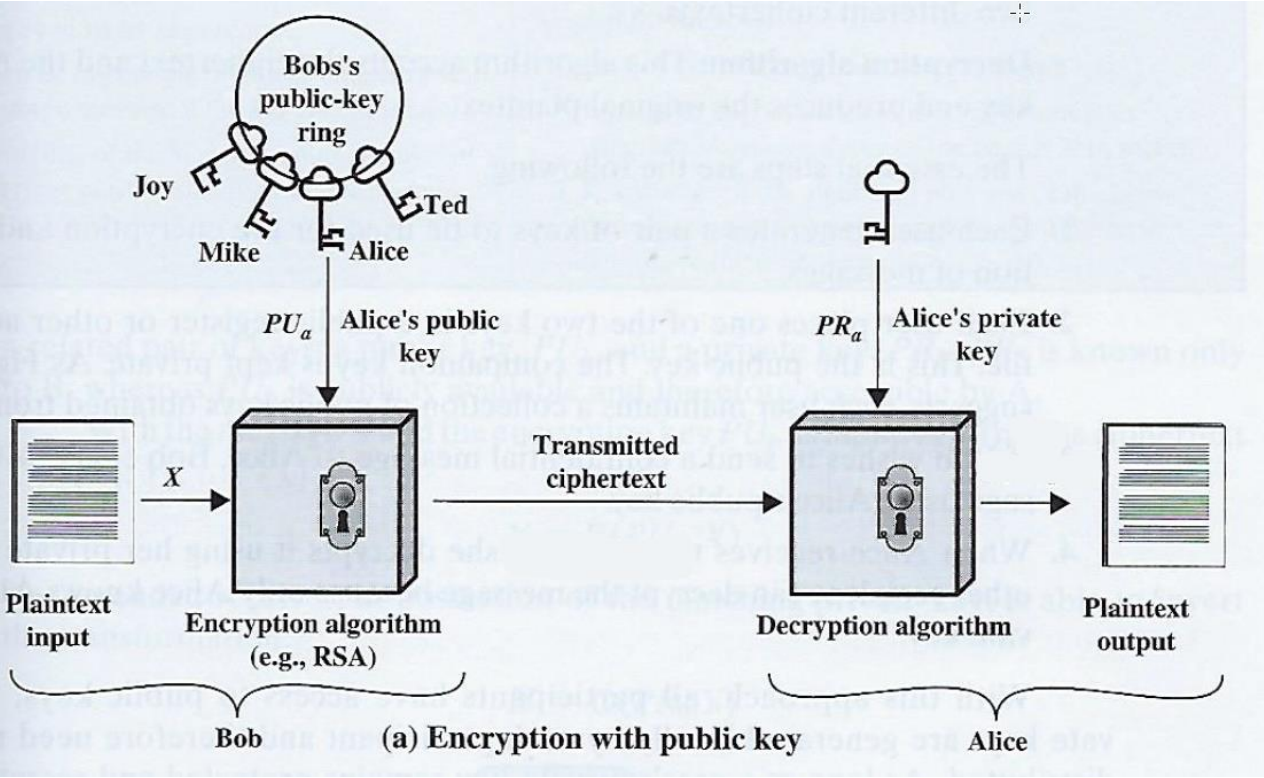
Symmetric and asymmetric and algorithms are often used together

- 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



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

Public Key Management



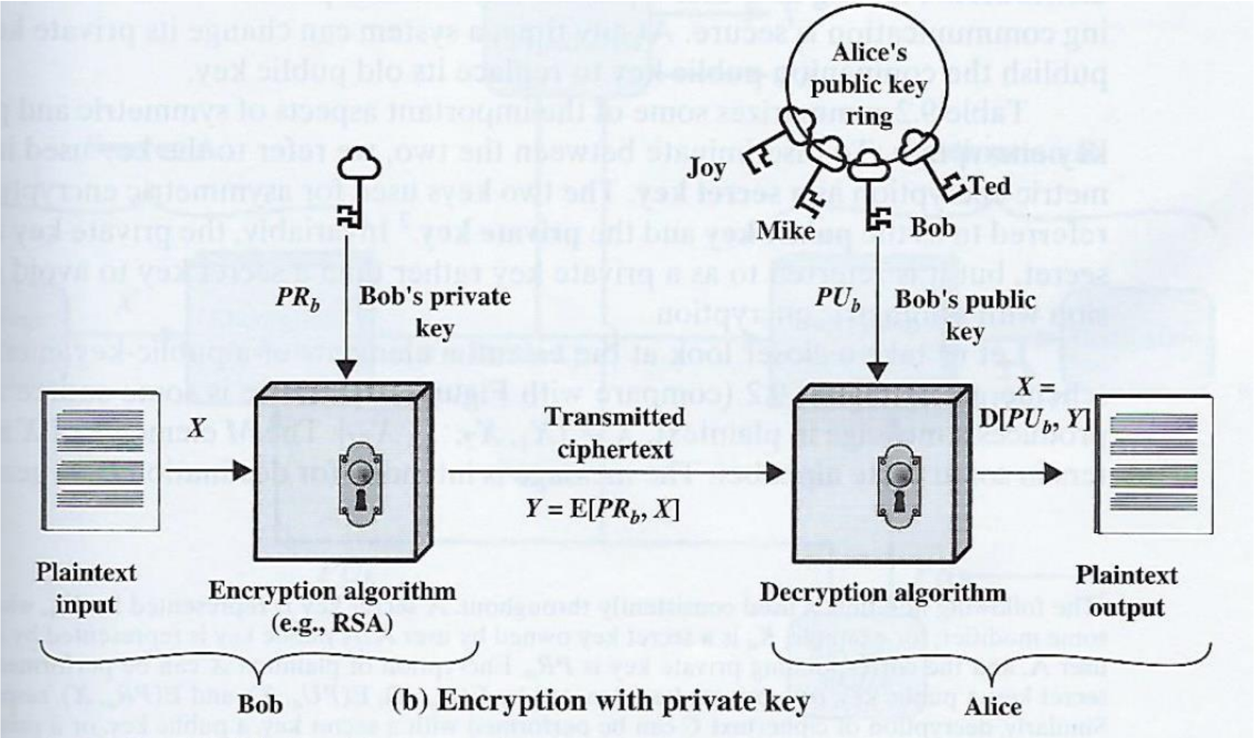
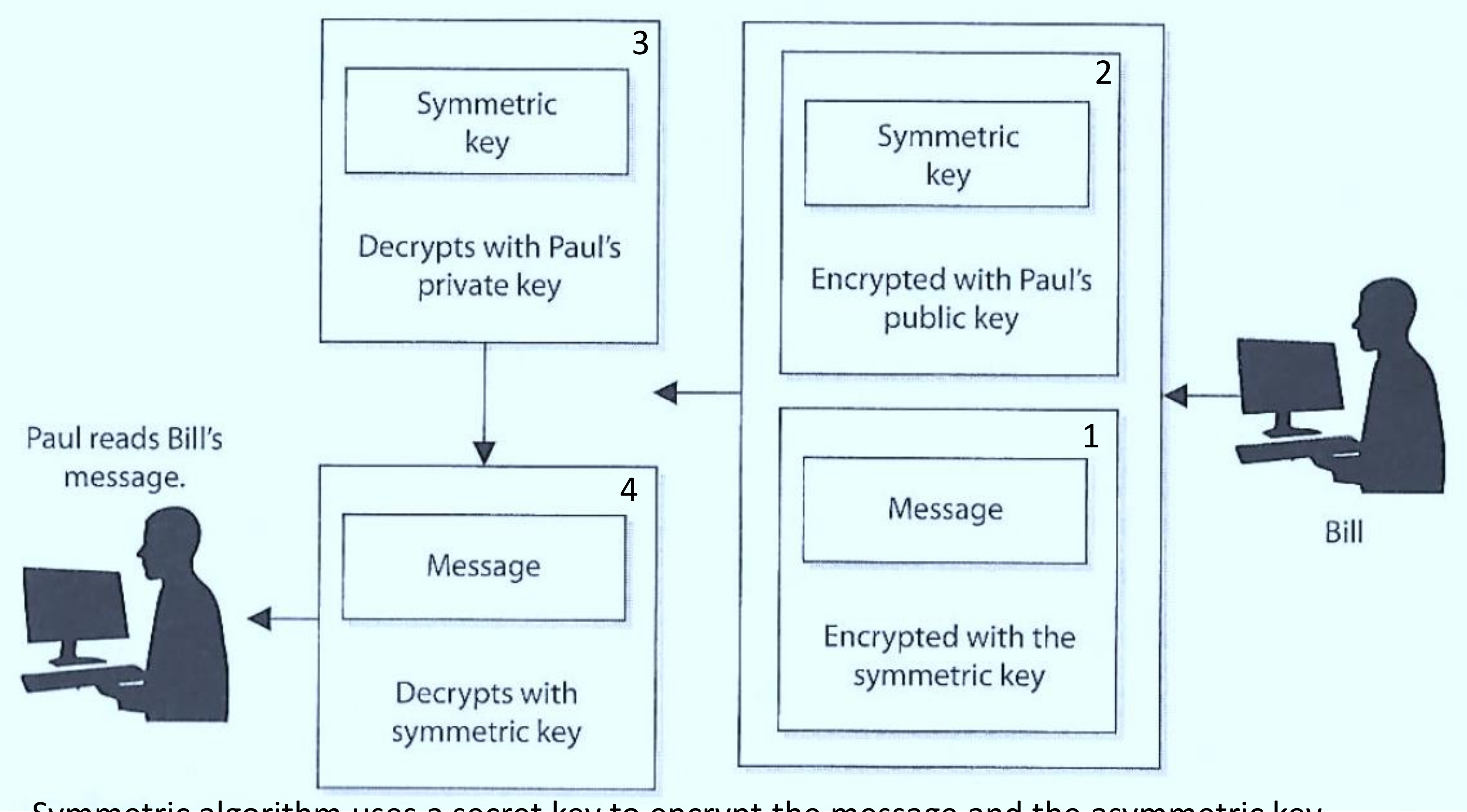


Figure 9.1 Public-Key Cryptography

Stallings, W. (2014) Cryptography and Network Security

Hybrid Encryption



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) <u>All-In-One CISSP Exam Guide</u>, 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

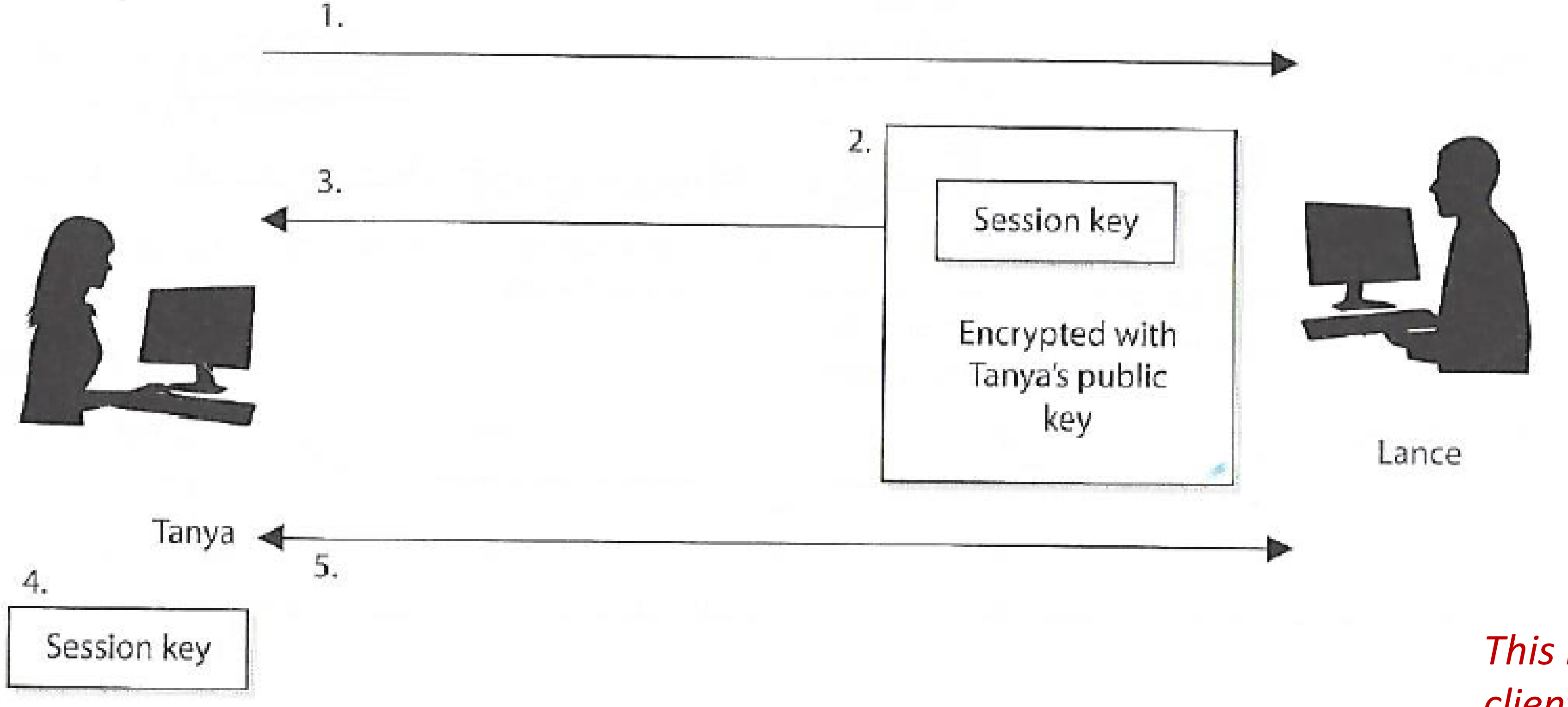
3. Why do we encrypt the message with the symmetric key rather than the asymmetric key?

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

<u>Single-use</u> 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.

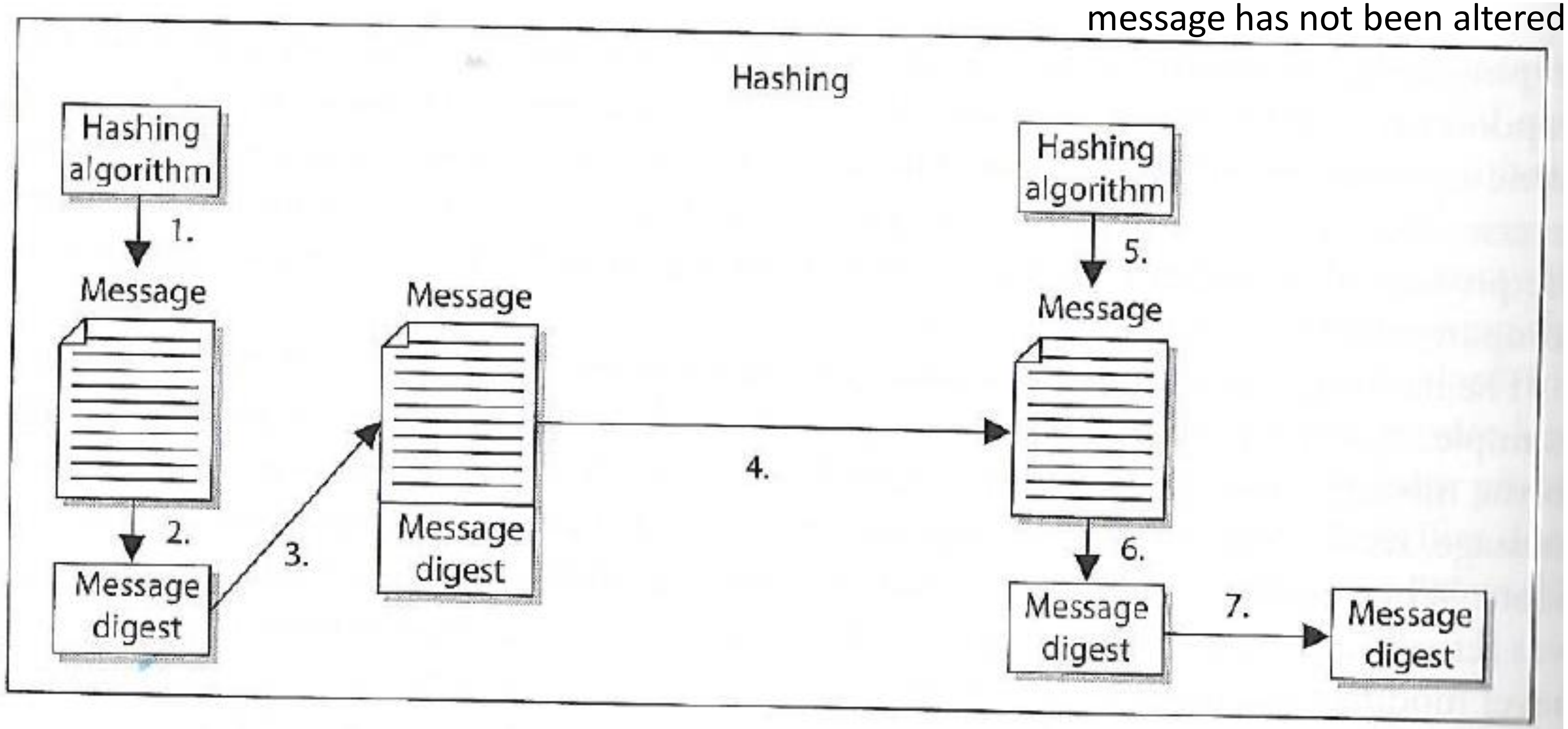
This is how secure web client applications communicate with server-side services

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

One-way Hash

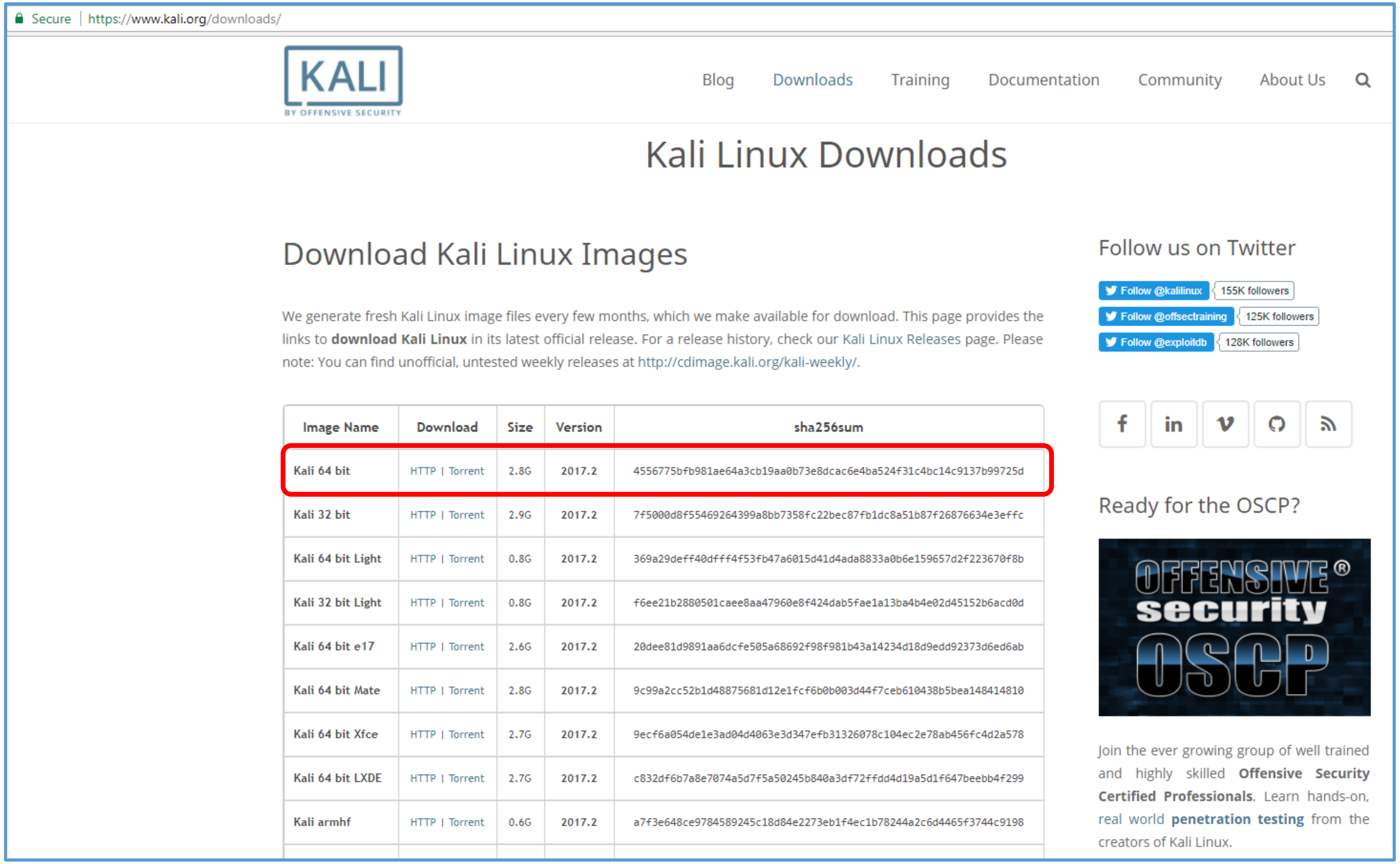
- Assures message **integrity**
- A function that takes a variable-length string (i.e. message) and produces a fixed-length value called a hash value
- Does not use keys

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

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

Follow @kalilinux 155K followers
Follow @offsectraining 125K followers
Follow @exploitdb 128K followers

Ready for the OSCP?

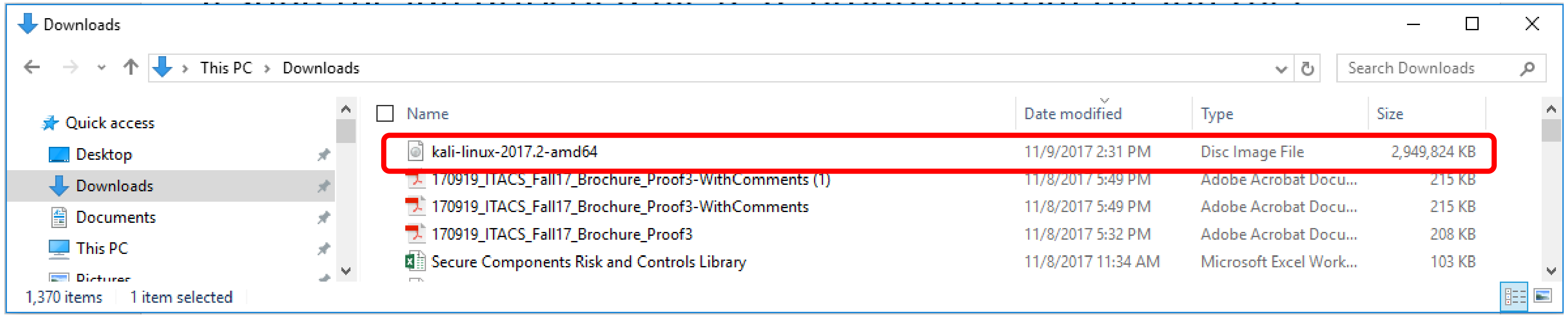
OFFENSIVE® security OSCP

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…

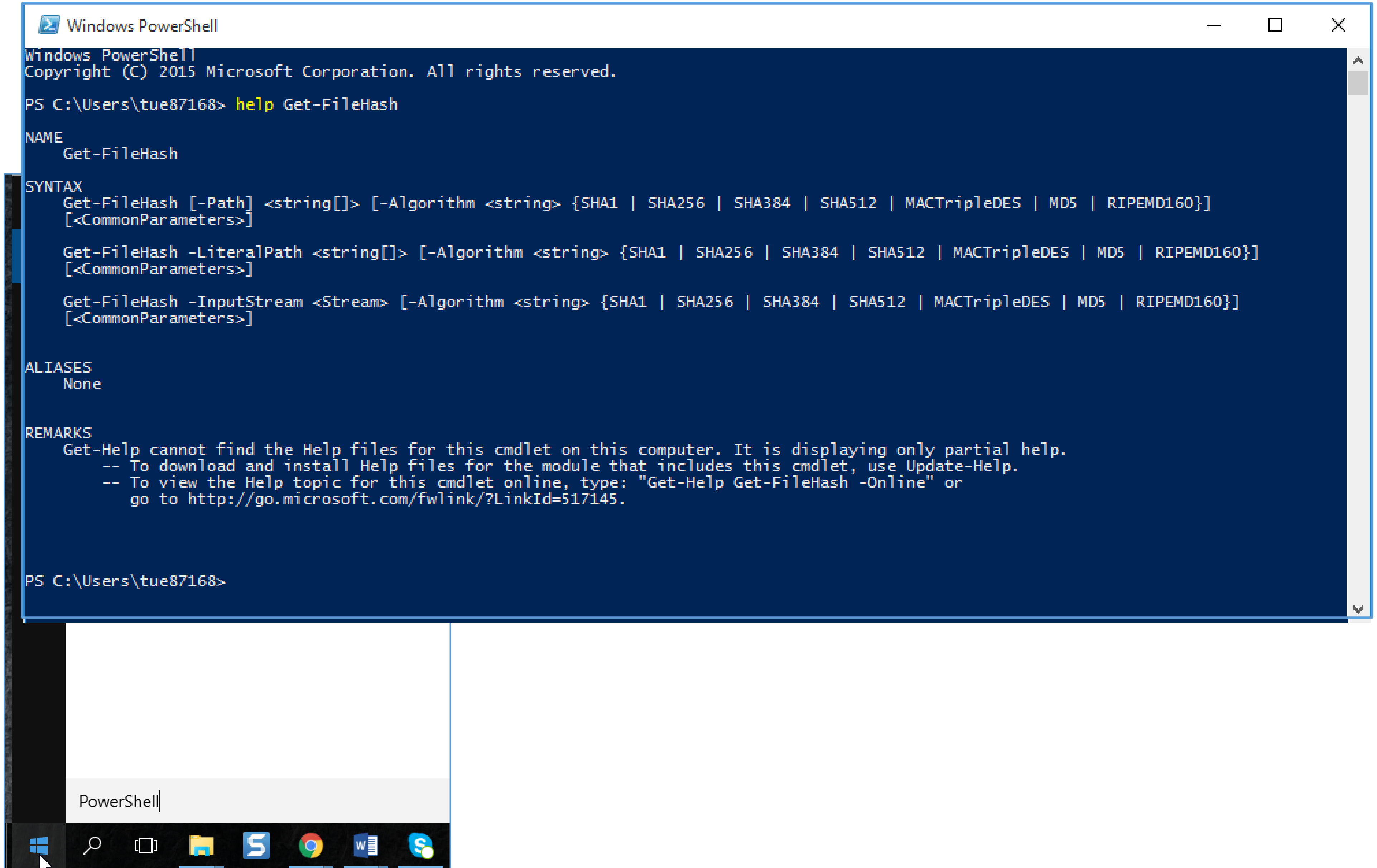
Testing the integrity of a file (e.g. program) from the internet…

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



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

One-way hash example...



One-way hash example…

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

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

PowerShell

```
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.

Windows PowerShell

```
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> _
```

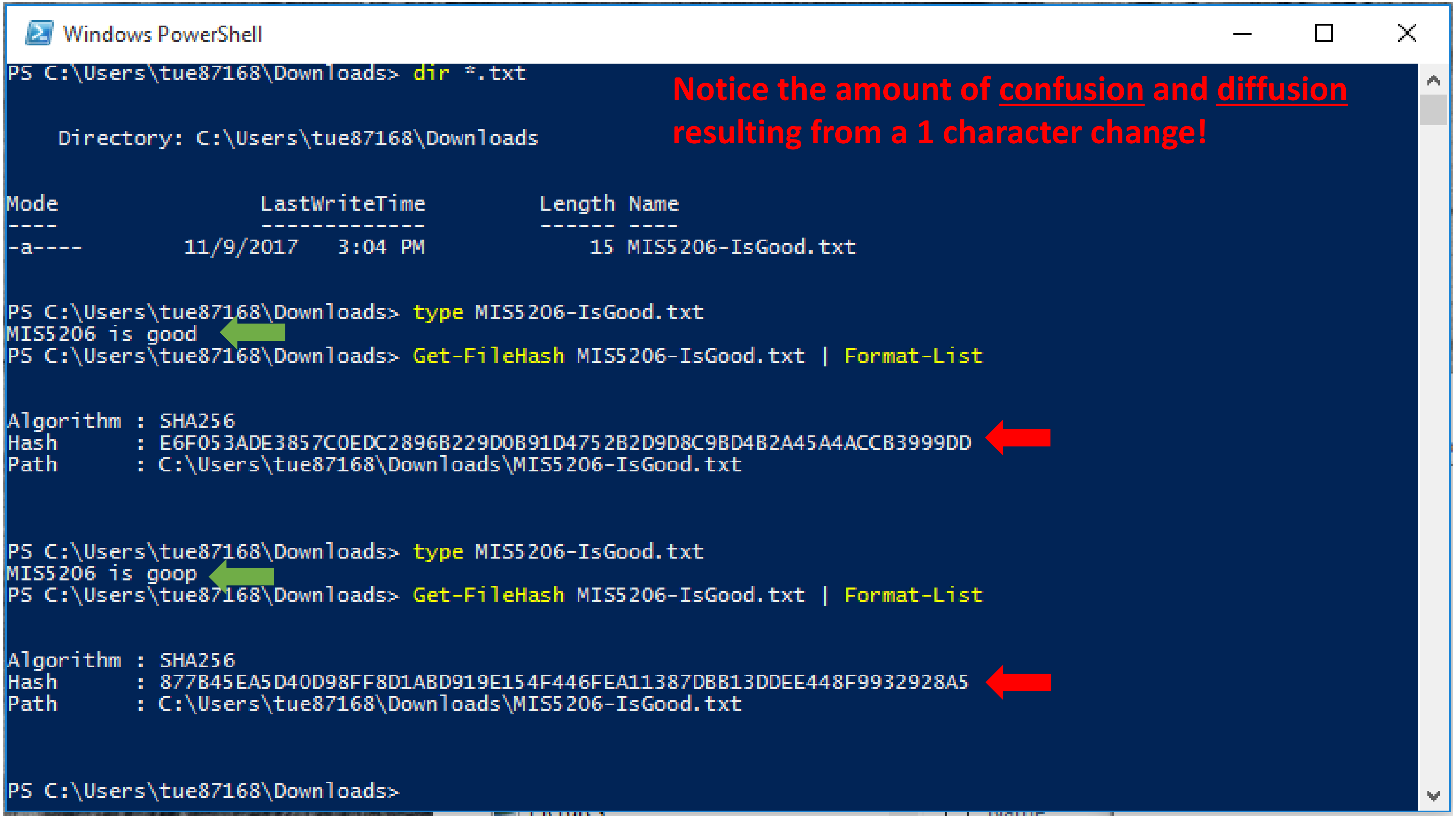
One-way hash example…

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

Windows PowerShell

```
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> _
```

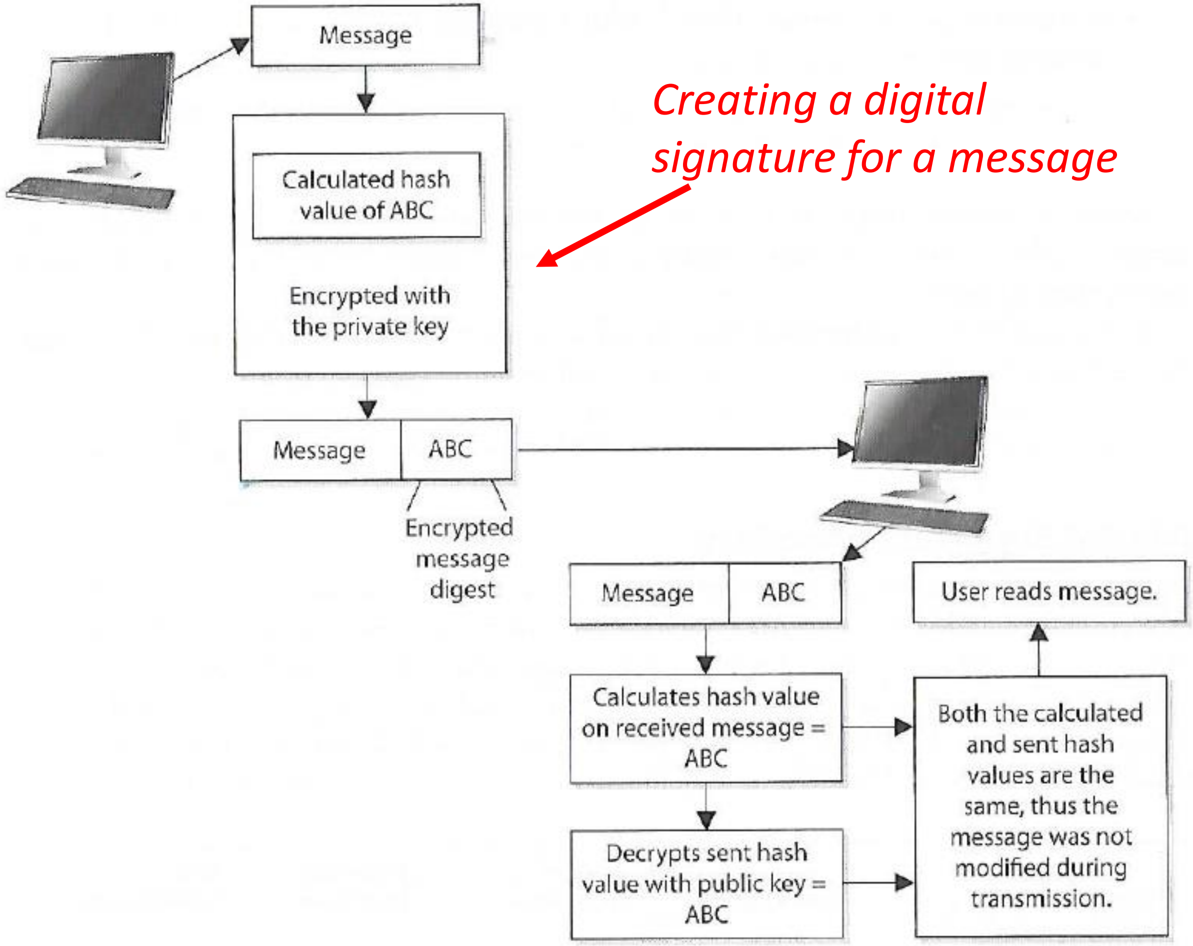
One-way hash example…




```
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



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

Strong cryptographic algorithms

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	Very weak	MD6, et. Al.
SHA-1	*Hashing – Integrity*	Rivest SHA Hash	512-bit processing Creates 160-bit hashes / digest	Weak	N/A
SHA-3	*Hashing – Integrity*	Hash	Creates 224-, 256-, 384-, or 512-bit hashes	Very Strong	

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

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)

- A list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted

Examples of Cryptanalysis Attacks

- Brute force
  - Trying all key values in the keyspace
- Frequency Analysis
  - Guess values based on linguistic analysis of frequency of occurrence of letters
- Dictionary Attack
  - Find plaintext based on common words
- Replay Attack
  - Repeating previous known values
- Known Plaintext
  - Format or content of plaintext available
- 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

Quiz

1. The review of router access control lists should be conducted during:
   a. An environmental review
   b. A network security review
   c. A business continuity review
   d. A data integrity review

1. The review of router access control lists should be conducted during:
   a. An environmental review
   b. A network security review
   c. A business continuity review
   d. A data integrity review

Quiz

2. During an audit of a telecommunication system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:
    a. Encryption
    b. Callback modems
    c. Message authentication
    d. Dedicated Leased lines

2. During an audit of a telecommunication system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:
    a. Encryption
    b. Callback modems
    c. Message authentication
    d. Dedicated Leased lines

Quiz

3. A digital signature contains a message digest to:
   a. Show if the message has been altered after transmission
   b. Define the encryption algorithm
   c. Confirm the identity of the originator
   d. Enable message transmission in a digital format

3. A digital signature contains a message digest to:
   a. Show if the message has been altered after transmission
   b. Define the encryption algorithm
   c. Confirm the identity of the originator
   d. Enable message transmission in a digital format

Quiz

4. Digital signatures require the:
    a. Signer to have a public key and the receiver to have a private key
    b. Signer to have a private key and the received to have a public key
    c. Signer and receiver to have a public key
    d. Signer and receiver to have a private key

4. Digital signatures require the:
    a. Signer to have a public key and the receiver to have a private key
    b. Signer to have a private key and the received to have a public key
    c. Signer and receiver to have a public key
    d. Signer and receiver to have a private key

Quiz

5. When using public key encryption to ensure confidentiality of data being transmitted across a network:
   a. Both the key used to encrypt and decrypt the data are public
   b. The key used to encrypt is private, but the key used to decrypt the data is public
   c. The key used to encrypt is public, but the key used to decrypt the data is private
   d. Both the key used to encrypt and decrypt the data are private

5. When using public key encryption to ensure confidentiality of data being transmitted across a network:
   a. Both the key used to encrypt and decrypt the data are public
   b. The key used to encrypt is private, but the key used to decrypt the data is public
   c. The key used to encrypt is public, but the key used to decrypt the data is private
   d. Both the key used to encrypt and decrypt the data are private

Quiz

6. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?
    a. A biometric, digitized and encrypted parameter with the customer’s public key
    b. A hash of the data that is transmitted and encrypted with the customer’s private key
    c. A hash of the data that is transmitted and encrypted with the customer’s public key
    d. The customer’s scanned signature encrypted with the customer’s public key

6. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?
    a. A biometric, digitized and encrypted parameter with the customer’s public key
    b. A hash of the data that is transmitted and encrypted with the customer’s private key
    c. A hash of the data that is transmitted and encrypted with the customer’s public key
    d. The customer’s scanned signature encrypted with the customer’s public key

Quiz

7. Email message authenticity and confidentiality is BEST achieved by signing the message using the:
    a. Sender’s private key and encrypting the message using the receiver’s public key
    b. Sender’s public key and encrypting the message using the receiver’s private key
    c. Receiver’s private key and encrypting the message using the sender’s public key
    d. Receiver’s public key and encrypting the message using the sender’s private key

7. Email message authenticity and confidentiality is BEST achieved by signing the message using the:
    a. Sender’s private key and encrypting the message using the receiver’s public key
    b. Sender’s public key and encrypting the message using the receiver’s private key
    c. Receiver’s private key and encrypting the message using the sender’s public key
    d. Receiver’s public key and encrypting the message using the sender’s private key

Quiz

8. Which of the following effectively verify the originator of a transaction?
   a. Using a secret password between the originator and the receiver
   b. Encrypting the transaction with the receiver's public key
   c. Using a portable document format (PDF) to encapsulate transaction content
   d. Digitally signing the transaction with the source's private key

8. Which of the following effectively verify the originator of a transaction?
   a. Using a secret password between the originator and the receiver
   b. Encrypting the transaction with the receiver's public key
   c. Using a portable document format (PDF) to encapsulate transaction content
   d. Digitally signing the transaction with the source's private key

Quiz

9. Which of the following is the MOST effective type of antivirus software to detect an infected application?
   a. Scanners
   b. Active monitors
   c. Hash-based integrity checkers
   d. Vaccines

9. Which of the following is the MOST effective type of antivirus software to detect an infected application?
   a. Scanners
   b. Active monitors
   c. Hash-based integrity checkers
   d. Vaccines

Agenda

- ✓Team Presentation Schedule
- ✓Cryptography and Cryptanalysis
- ✓Terminology
- ✓Symmetric Cryptography
- ✓Asymmetric Cryptography
- ✓Hashing and Digital Signature
- ✓Public Key Infrastructure
- ✓Cryptanalysis Attacks
- ✓Quiz

Protecting Information Assets
- Unit# 11 -

Cryptography, Public Key Encryption and Digital Signatures