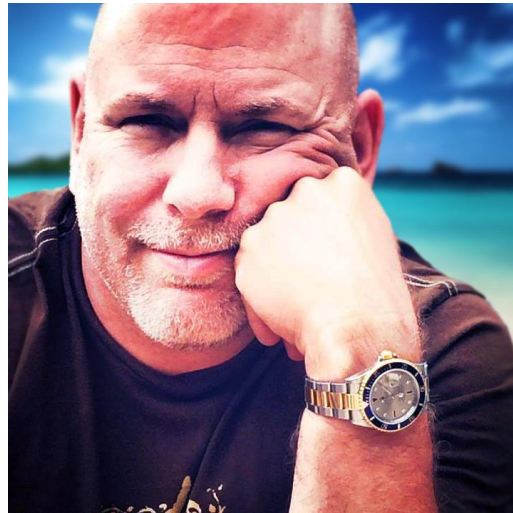


CompTIA Security+ (SY0-401) Cryptography

General Cryptography Concepts



Christopher Rees

@cdrees | <https://www.linkedin.com/in/cdrees>

Series TOC

- CompTIA Security+ (SY0-401) Network Security
- CompTIA Security+ (SY0-401) Compliance and Operational Security
- CompTIA Security+ (SY0-401) Threats and Vulnerabilities
- CompTIA Security+ (SY0-401) Application, Data and Host Security
- CompTIA Security+ (SY0-401) Access Control and Identity Management
- **CompTIA Security+ (SY0-401) Cryptography**

Module Overview

- Symmetric vs. asymmetric
- Session keys
- In-band vs. out-of-band key exchange
- Fundamental differences and encryption methods
 - Block vs. stream
- Transport encryption
- Non-repudiation
- Hashing
- Key escrow
- Steganography
- Digital signatures
- Use of proven technologies
- Elliptic curve and quantum cryptography
- Ephemeral key
- Perfect forward secrecy

Cryptographic Terminology

- Cryptography – the practice and study of **hiding** information
- Cryptanalysis – discovering some **weakness or insecurity** in a cryptographic scheme
- Encryption – the method of **transforming data** (plaintext) into an unreadable format
- Plaintext – the (readable) format of data **before** being encrypted
- Ciphertext – the “scrambled” format of data **after** being encrypted

Cryptographic Terminology

- Decryption – the method of turning **cipher text** back into **plaintext**
- Encryption algorithm – a set of **rules** or procedures that defines how to encrypt and decrypt data (also known as encryption cipher)
- Key – **value** used in the encryption process to encrypt and decrypt (cryptovariable)

Cryptography History

- Cryptography is over 4,000 years old and predates computers, electronics or any technology
- Early cryptography relied on methods to simply scramble text – otherwise known as a cipher
 - Substitution
 - Transposition

Substitution Cipher

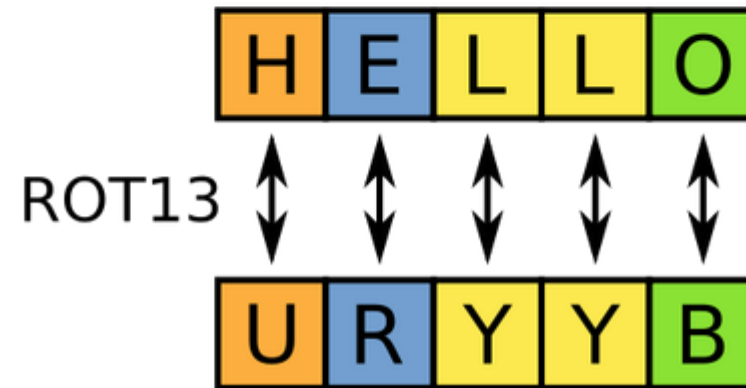
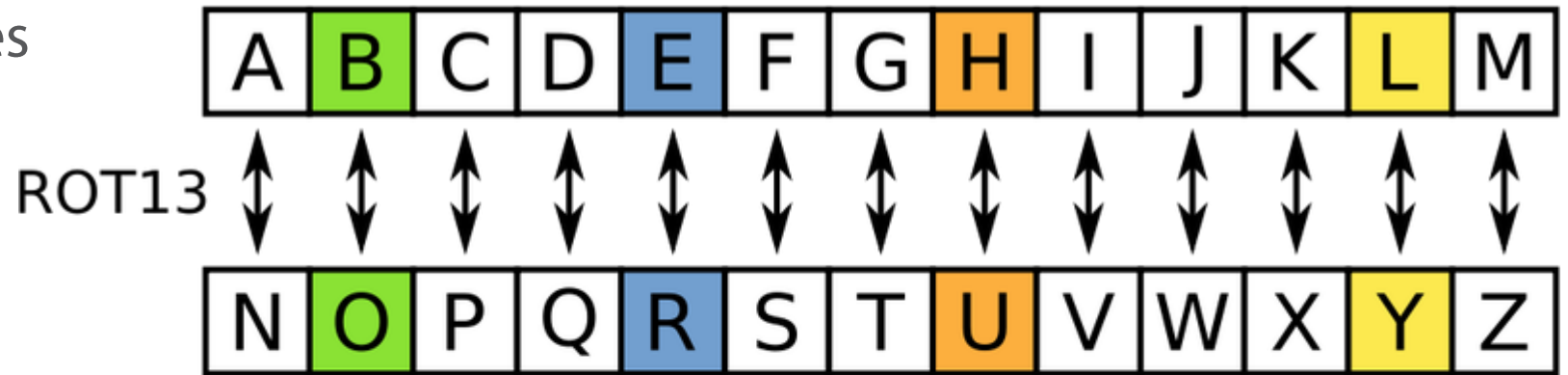
- Changing one character for another
- Caesar cipher (sometimes known as a shift-cipher)
 - Process of **shifting** all the letters a certain number of spaces in the alphabet

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
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

Alphabet shifted by 3 spaces.

ROT-13

- Substitution Cipher
 - Rotates letters 13 spaces



Vigenère Table

- Multi-alphabet substitution
 - Secret** keyword only **you** and the **other person** knows
 - Line up the single-line phrase you wish to send and **repeat** the keyword underneath until it fills all the spaces

Your Message

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

Your Keyword

Vigenère Example

```
PluralsightSecurityPlusRocks <-Message  
comptiacomptiacomptiacomptia <-Keyword  
rzggttskutilmcwfuirxlgddvss <-Encrypted
```

PluralsightSecurityPlusRocks <-Message
comptiacomptiacomptiacomptia <-Keyword
rzggttskutilmcwfuirxlgddvss <-Encrypted

“C” from keyword (comptia)

“P” from message (pluralsig...)

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

PluralsightSecurityPlusRocks <-Message
comptiacomptiacomptiacomptia <-Keyword
rzggttskutilmcwfuirxlgddvss <-Encrypted

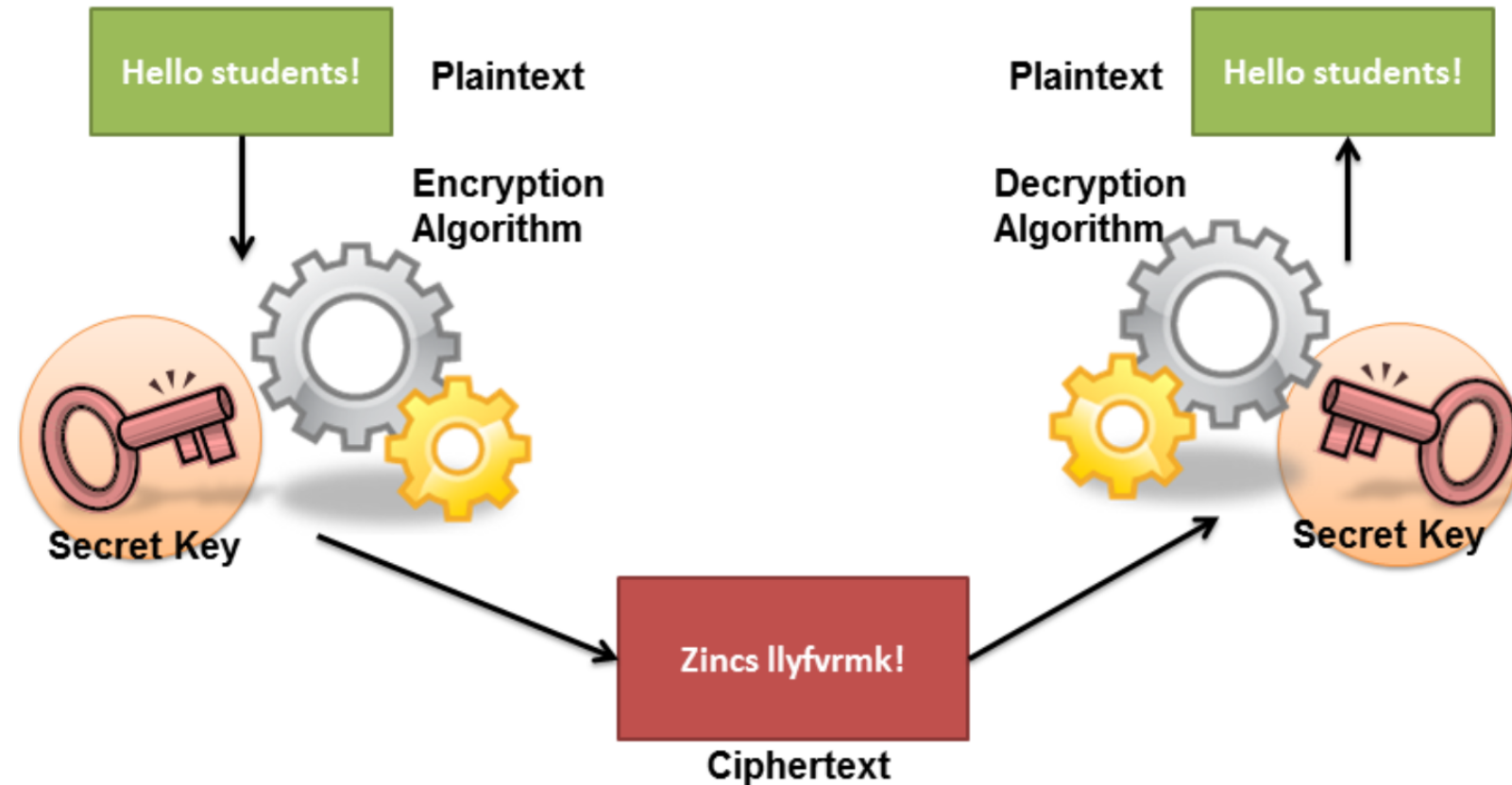
“C” from keyword (comptia)

“P” from message (pluralsig...)

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

Symmetric vs. Asymmetric

- Symmetric encryption – uses the **same** key to encrypt and decrypt a piece of data



Same key used for both operations

Symmetric Encryption

- Same key is used for **both** encryption and decryption
 - Often referred to as shared key or secret key encryption
- **Key management** is biggest concern
 - Both parties must know the secret key
 - Difficult to prove identity (multiple people could know the key)
- Symmetric is **faster** than asymmetric
 - Strength is affected by the length of the key
 - Number of iterations through the algorithm

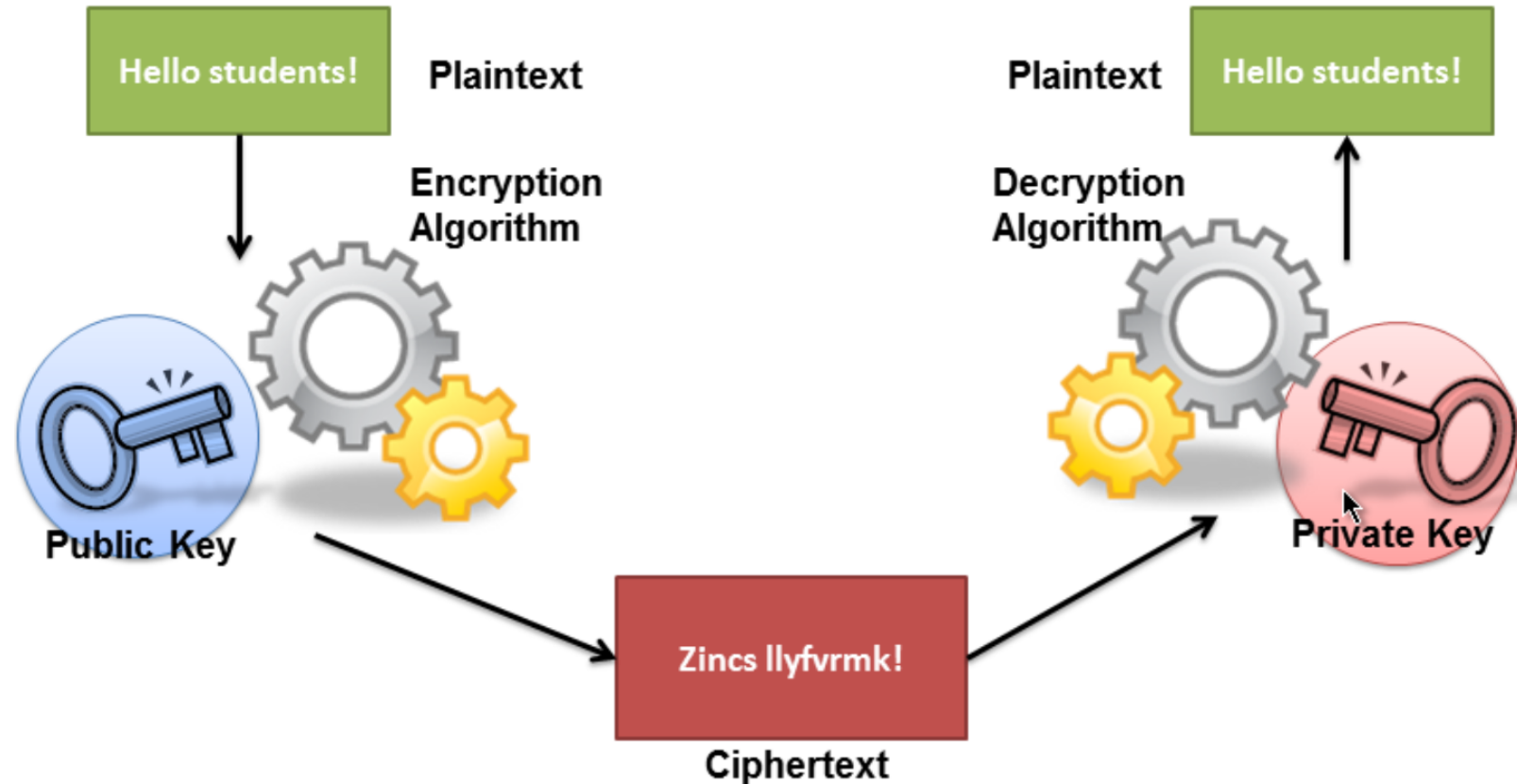


Symmetric vs. Asymmetric

- Asymmetric Encryption uses a **two-key** (Public Key / Private Key) system



Two keys – One public, one private



Asymmetric Encryption

- **Key pair** is used: one key for encryption and the other for decryption
 - Public key is made **publicly available**
 - Private key must be **kept secret**
- Either key can encrypt and either key can decrypt
 - Encrypt with the public key and decrypt with the private key
 - Encrypt with the private key and decrypt with the public key
- Message encrypted can not be decrypted with the same key (public -> public or private -> private)



Session Keys

- **Single-use** symmetric key used for encrypting all communication in one communication session
 - Symmetric encryption is faster than asymmetric encryption
 - Asymmetric keys can be used to encrypt the session keys



In-band vs. Out-of-Band Key Exchange

- Out-of-band Key Exchange
 - **Not** sent over the network
 - Needs to be delivered via traditional/manual means (in-person, telephone, courier, etc)
- In-band Key Exchange
 - Done **over the network** as the communication session is established
 - Created in real-time then typically discarded once the session is over

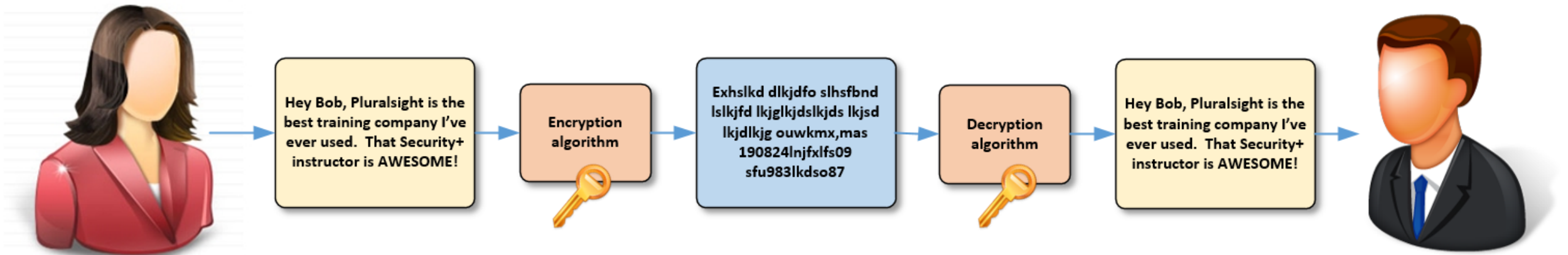
Fundamental Differences and Encryption Methods

Block vs. Stream - Both are **symmetric** encryption methods

- Block cipher
 - Encrypts in **chunks** (blocks) of data at a time
- Stream cipher
 - Encrypts **one bit** at a time

Block Cipher

- Block Ciphers
 - **Fixed length** group of bits (blocks)
 - Each block of plaintext has an equivalent size of block ciphertext
 - Transformation is controlled by a symmetric **Secret Key**
 - Decryption uses the secret key to transform back into plain text



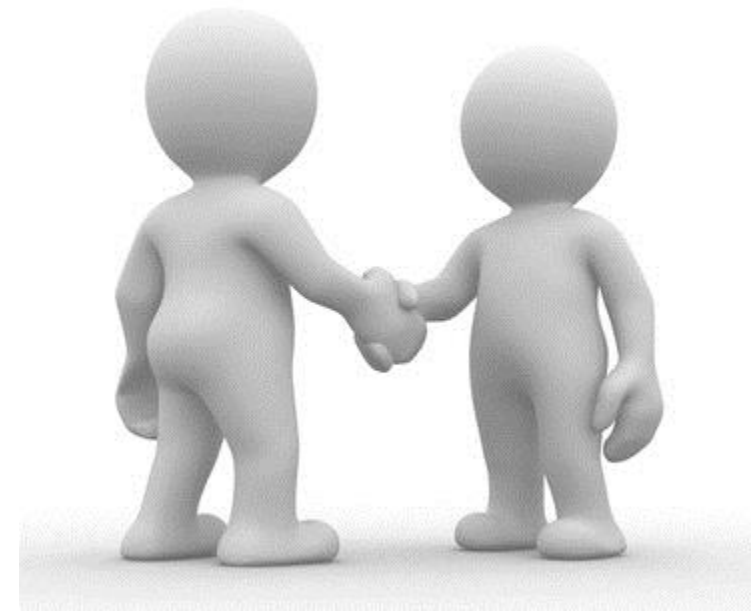
Stream Cipher

- Stream Ciphers
 - Encryption takes place bit by bit using a **pseudorandom** cipher digit stream (keystream)
 - In a stream cipher each plaintext digit is encrypted **one at a time** with the corresponding digit of the keystream, to give a digit of the ciphertext stream.



Transport Encryption

- SSL/TLS and HTTPS
 - Secure Sockets Layer / Transport Layer Security and Hypertext Transfer Protocol Secure
- SSL/TLS allows for **secure communication** over an unsecure network
 - Offers protection against eavesdropping, tampering and message forgery
- TLS uses a **handshake** between both parties to authenticate and agree on how to communicate



Transport Encryption

- SSL/TLS Security Considerations
 - Only as strong as the ciphers and hashing **agreed upon by both parties**
 - MiTM (Man in the Middle) attacks exist that force both parties to agree to use unsecure protocols



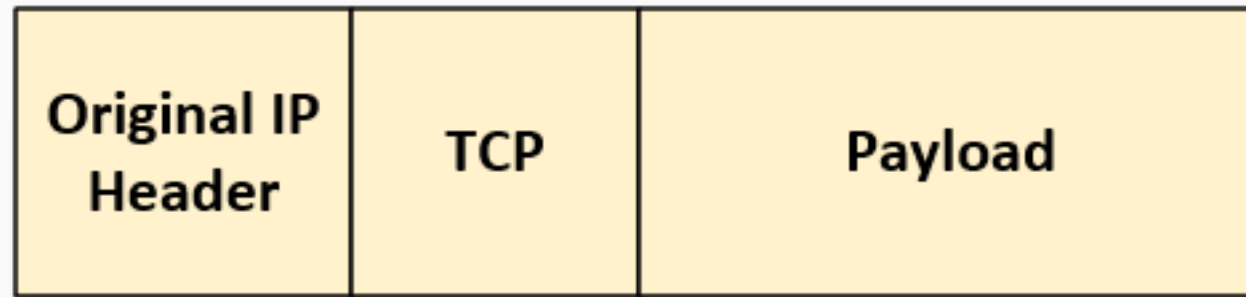
Transport Encryption

- SSH (Secure Shell)
 - Secure remote sessions, file transfers, tunneling, port forwarding and more
 - Same security considerations as SSL/TLS



Transport Encryption

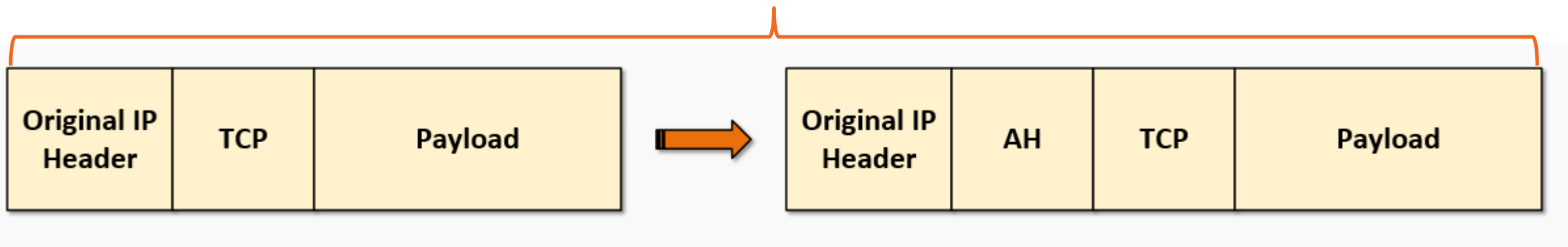
- IPsec (Internet Security Protocol)
 - Authentication Header (AH)
 - Provides authentication and integrity



Transport Encryption

- IPSec (Internet Security Protocol)
 - Authentication Header (AH)
 - Provides authentication and integrity

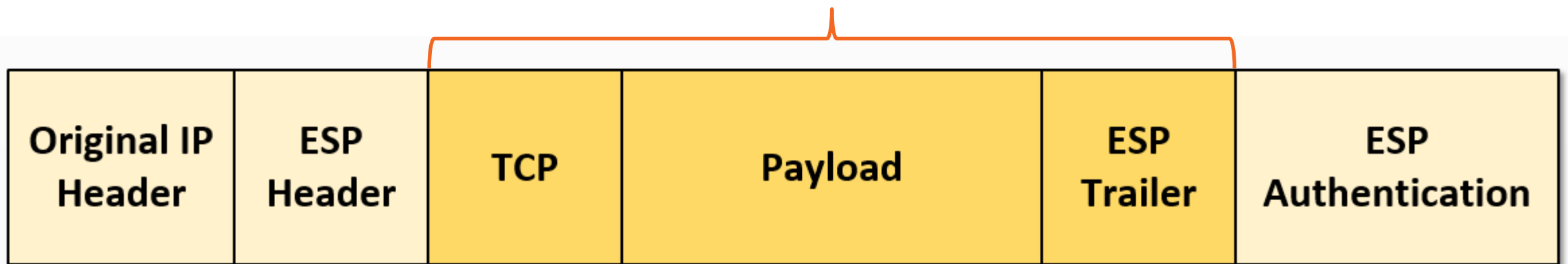
No Encryption as the AH only offers **Integrity**



Transport Encryption

- IPsec
 - Encapsulating Secure Payload (ESP)
 - Provides confidentiality along with option integrity checking
 - Adds a header, trailer and integrity check value (ICV)

Encrypted which provides **data confidentiality**



Note: Transport Mode

Non-Repudiation

- Assurance that the author of a message **cannot later refute ownership**
 - Asymmetric encryption functions on the premise of a secret key **only the sender** would know
- Does not prevent someone from compromising a user's secret key and encrypting a message as them



Hashing

- Mathematical algorithm applied to a file **before** and **after** transmission
 - If anything within the file changes the hash will be **completely** different
- MD5, SHA1 and SHA2
- Example (SHA1)
 - Pluralsight really is the best training on the planet!
 - **052ff1f85f58f53d0ad17ef5907ad5fb883d4136**
 - Pluralsight really is the best training on the planet
 - **2f5f50d07cff1a7a15dcfabd793d12d6469ebebc**

Key Escrow

- Keys needed to decrypt encrypted data are held in escrow to enable an **authorized third party** to access those keys
 - Referred to as a “fair” cryptosystem
- Recovery Agents can be used to allow access to older keys

A man with dark hair and black-rimmed glasses is peeking over a white surface. His hands are visible on the surface, one on each side of his head. An orange speech bubble with white text is positioned to the right of his head.

**Trust Me!
I'm here to Help**

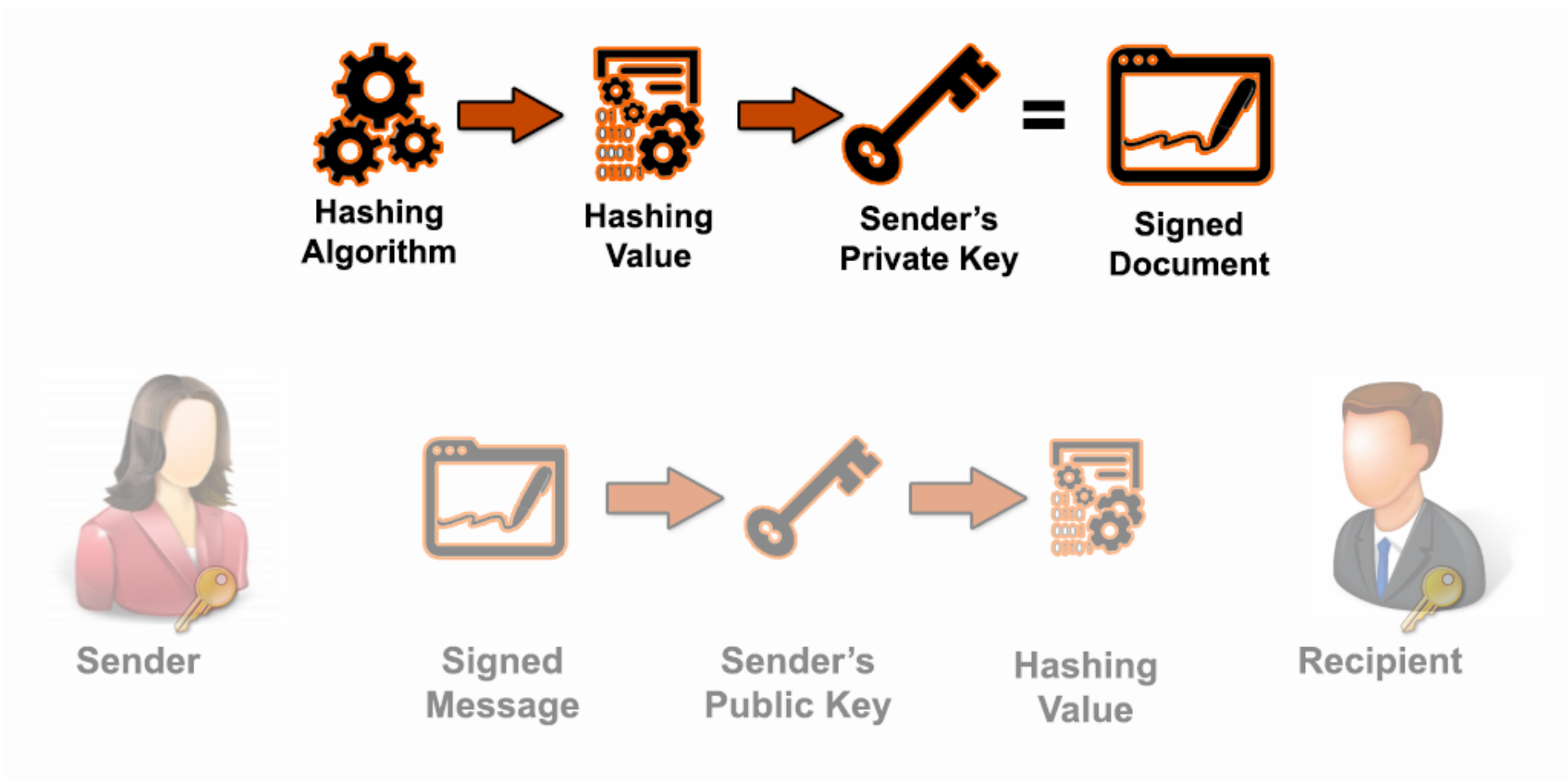
Steganography

- Hiding something **inside** of something else
 - Documents could be hidden inside of other documents
 - Mp3 files
 - Image files
 - Video files



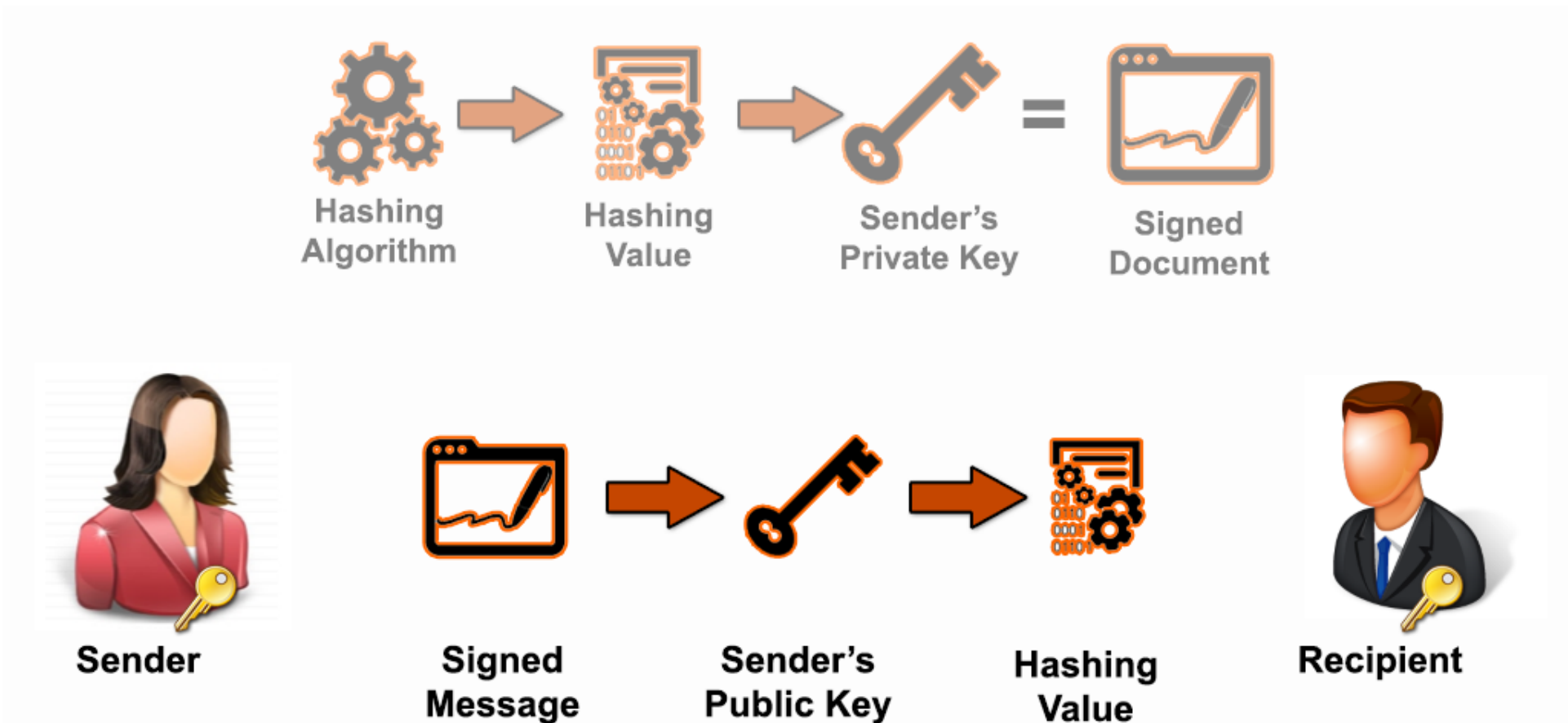
Digital Signatures

Asymmetric encryption using public-key / private-key (PKI)



Digital Signatures

Asymmetric encryption using public-key / private-key (PKI)



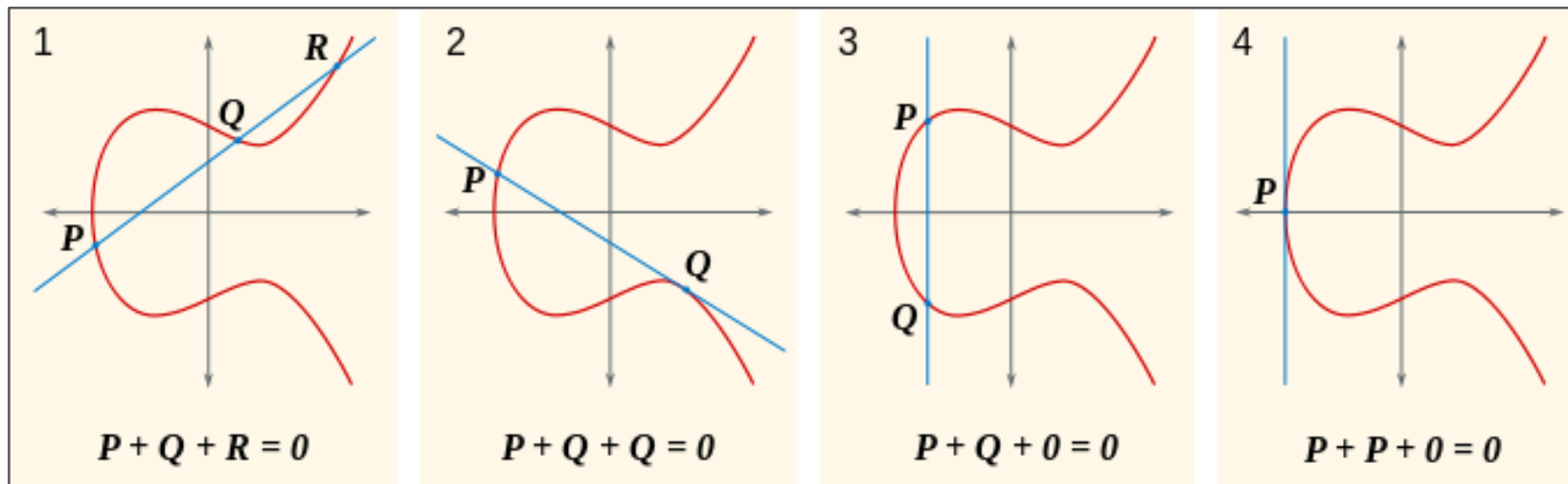
Use of Proven Technologies

- Kerckhoffs's Principle
 - States that the **security** of an algorithm should depend **only** on the **secrecy of the key** and not on the secrecy of the algorithm itself
 - All of the generally used encryption algorithms are **publicly accessible**
 - They've been vetted by the security community for flaws, etc



Elliptic Curve Cryptography

- Elliptic Curve Cryptography (ECC)
 - Asymmetric encryption that uses **algebraic structure of elliptic curves**
 - Strong encryption using **smaller key size**
- Asymmetric encryption normally requires a **large** amount of resources
 - ECC can achieve **same** level of security with less resources



Quantum Cryptography

- The use of **quantum mechanical properties** to perform cryptographic tasks
 - The very act of **eavesdropping** disturbs the properties of the communication
 - Provides “unconditional security”



Quantum Cryptography

- Quantum Key Distribution (QKD)
 - Using quantum communication to establish a **shared key** between two parties
 - Third party (eavesdropper) can't **access or disturb** the data without it being noticed by sender/recipient



Ephemeral Key

- Temporary key that is used once
 - Can be **reused** during a single communication session
 - Can also be used to **derive an additional** key that is used for subsequent communication



Perfect Forward Secrecy

- Session keys that are derived from a set of long-term keys, yet discreet in nature
 - If one of the long term keys is compromised it **doesn't compromise** the session key or the data it protects
 - Keys used to protect data aren't used to derive any **additional keys**
 - If the key used to protect data was derived from some other keying material, the material **must not be used** to derive any additional keys



Module Review

- Symmetric vs. asymmetric
- Session keys
- In-band vs. out-of-band key exchange
- Fundamental differences and encryption methods
 - Block vs. stream
- Transport encryption
- Non-repudiation
- Hashing
- Key escrow
- Steganography
- Digital signatures
- Use of proven technologies
- Elliptic curve and quantum cryptography
- Ephemeral key
- Perfect forward secrecy