Lesson Proper for Week 15

ENCRYPTION AND CERTIFICATES

Encryption is the process of encoding data that is at rest or in transit to prevent unauthorized access and that only the right entities can see it. Encryption hides data or the contents of a message in such a way that the original information is then recovered through a corresponding decryption process. This is achieved by taking the original data and mathematically encoding it using an encryption key.

How does encryption work?

An encryption algorithm is used to encrypt the data that is to be communicated or stored (also known as plaintext) into unreadable or encrypted data. Encrypted data (also known as cipher text) can only be read once decrypted.

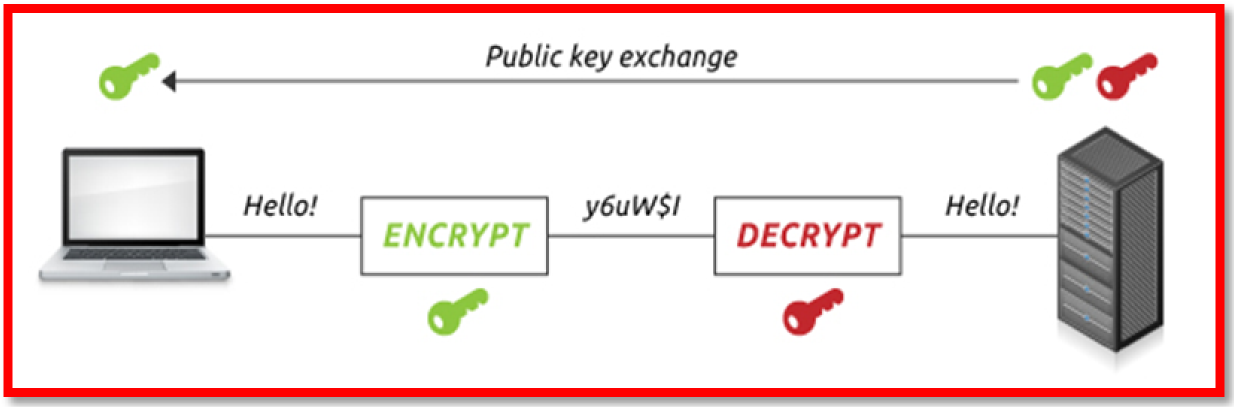
For example, at the sender's end of the conversation an encryption key is used to encrypt the data to be communicated, while a decryption key is used at the receiving end to decode encrypted data.

Why is encryption needed?

Encryption helps protect private information, sensitive data, and enhance the security of outgoing data or data in transit. Encryption hides sensitive data from people who should not be able to see it, and ultimate purpose is to protect the confidentiality of digital data stored on a computer or communicated over a network.

TYPES OF ENCRYPTION

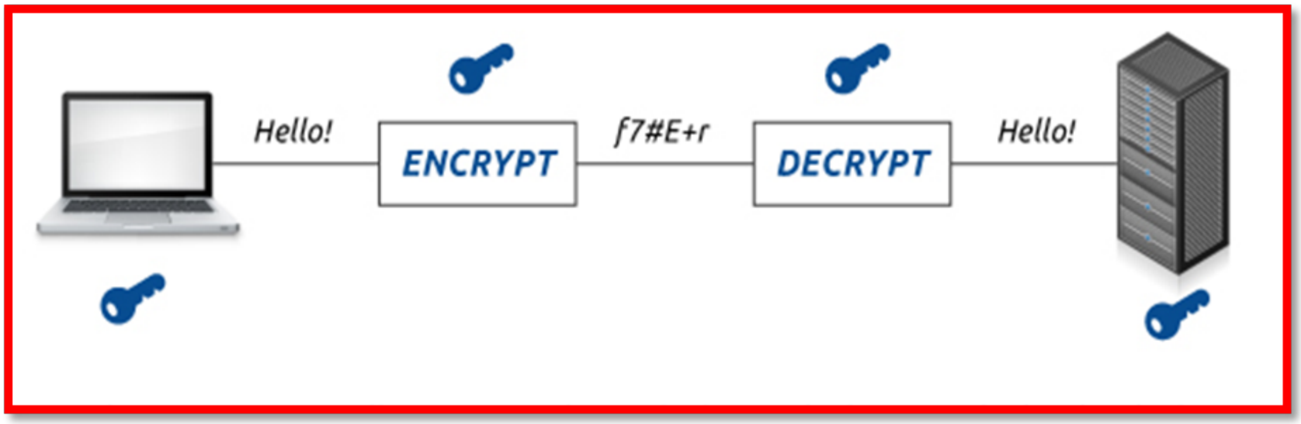
1. **Asymmetric encryption** (or public-key cryptography) uses a separate key for encryption and decryption. Anyone can use the encryption key (public key) to encrypt a message. However, decryption keys (private keys) are secret. This way only the intended receiver can decrypt the message.



Pros: Eliminates the preliminary exchange of secret keys, public keys can be shared with anyone, provides the underlying architecture used in digital certificates, digital signatures, and Public Key Infrastructure

Cons: Much slower than private key encryption, requires greater computational power.

2. **Symmetric encryption** (or pre-shared key encryption) uses a single key to both encrypt and decrypt data. Both the sender and the receiver need the same key to communicate.



Pros: Fast, easily implemented by hardware, commonly used for bulk data encryption.

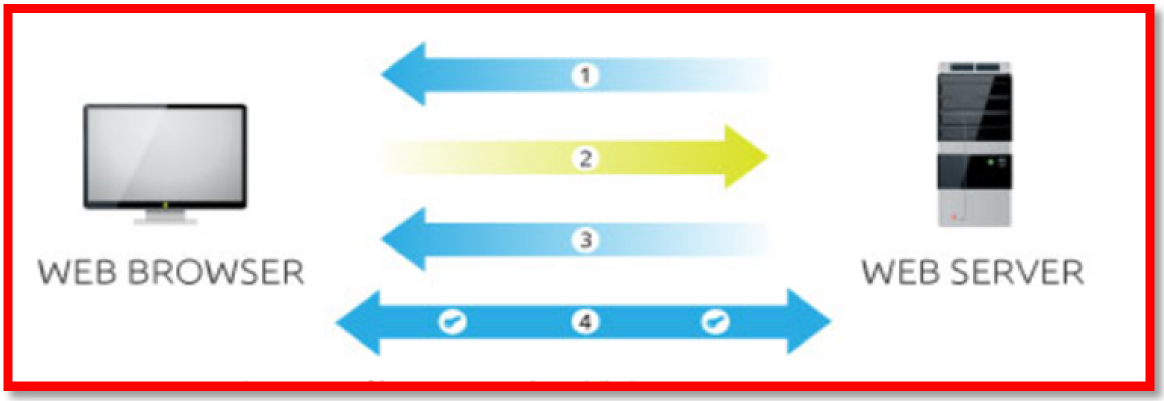
Cons: Complications with distribution and control of private keys, e.g. anyone with your key can decrypt your messages even if it wasn't intended for them.

SECURE SOCKET LAYER AND THE ASYMMETRIC AND SYMMETRIC ENCRYPTION

SSL (Secure Sockets Layer)

A standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).

It allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely.



1. **Server** sends a copy of its asymmetric public key.

2. **Browser** creates a symmetric session key and encrypts it with the server's asymmetric public key. Then sends it to the server.

3. **Server** decrypts the encrypted session key using its asymmetric private key to get the symmetric session key.

4. **Server** and **Browser** now encrypt and decrypt all transmitted data with the symmetric session key. This allows for a secure channel because only the browser and the server know the symmetric session key, and the session key is only used for that session. If the browser was to connect to the same server the next day, a new session key would be created.

How is encryption used in communications?

Protocols such as TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer) are cryptographic protocols used to provide secure communications over a network. Both use certificates and asymmetric cryptography to authenticate the counterpart in a conversation and then negotiate a symmetric session key. The symmetric session key is then used to encrypt data during the conversation.

TLS allows for data and message confidentiality as well as message authentication. Versions of TLS and SSL are used in applications such as email, instant messaging, and web browsing.

DIGITAL CERTIFICATES AND DIGITAL SIGNATURES

Digital Signature

Allows a recipient to establish whether a message was created by a known sender (authentication), that the message was not altered in any way during transit (integrity), and that the sender cannot deny having sent the message (non-repudiation).

A digital signature is therefore an authentication mechanism that acts as the equivalent of a handwritten signature, and that is attached to the message sent by a sender.

A digital signature scheme typically consists of three algorithms:

§ A key generation algorithm that generates a private key and a corresponding public key.

§ A signing algorithm that produces a signature for a specific message and private key.

§ A signature verifying algorithm that access or rejects the message’s claim to authenticity based on the message, the public key, and the digital signature.

*The authenticity of a digital signature can be verified using the public key for a signature generated from a message and a private key, AND it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. Digital signatures are used in some types of digital certificates

Digital Certificate

A public key certificate or digital certificate, is an electronic document that is used to prove the ownership of a public key. A certificate includes information about the public key, information about the owner's identity, and the digital signature of an entity that attests to the correctness of the certificate's contents

If a signature is deemed valid and the person or entity examining the certificate trusts the signer, then they know they can use that public key to communicate with its owner. By certifying the ownership of a public key by the named subject of the certificate, the digital certificate can help verify whether a sender is who they claim to be.

A certificate establishes authenticity by guaranteeing that the data it contains cannot be forged. Once trust is established, the information in the certificate will confirm that we are communicating with the right entity or person.

SIGNER

In a model of where a trust relationship is established, the entity that verifies the certificates contents is known as the **signer.** In a ***Public Key Infrastructure scheme***, the ***signer*** is a Certificate Authority (CA), an entity or company that charges customers a fee to issue digital certificates for them.

In this relationship of trust scheme, the signer is trusted by the entity examining the certificate, and they know they can use that specific key to communicate with its owner. The CA is known the trusted third party, trusted by both the owner of the certificate and the party relying on the certificate.

Examples of companies that issues digital certificates are Comodo and Symantec (formerly VeriSign). Users can also issue self-signed certificates, without the need of going through a CA.

How are digital certificates issued?

Digital certificates can be issued in a variety of ways:

§ A Certificate Authority (CA) can issue certificates.

§ Operating systems have embedded tools to create certificates. For example, Windows Server has the ability to create certificates through Active Directory Certificate Services. Certificates can then be issued to Windows users and Windows-based servers and computers.

§ Utilities are also available for creating unmanaged certificates, e.g. From Microsoft utilities such as SelfSSL.exe. With a self-signed certificate, the certificate is signed by the same entity whose identity it certifies.

How are certificates used?

One of the most common uses of certificates is for HTTPS-based web sites. A web browser will validate that a web server is authentic so that the user feels secure in that communications with the web sites are protected and the web site is who it claims to be. In this scenario, certificates are used by the TLS protocol to prevent attackers from impersonating a secure website.

Another use is during the encryption of email messages that rely on public key cryptography and authentication: each user can publish a public key that others can use to encrypt messages to them (digital signing and message encryption using certificates).

◀ Preliminary Activity for Week 15

Jump to... ⌄

Analysis, Application, and Exploration for Week 15 ▶

Navigation

Home
Dashboard
Site pages
My courses
Capstone Project 1
Network Attacks: Detection, Analysis & Counter...
Participants
General
12 - Midterm Examination
14 Search Engines
15 Encryption And Certificates
Preliminary Activity for Week 15
Lesson Proper for Week 15
Analysis, Application, and Exploration for Week 15
Generalization for Week 15

        - Evaluation for Week 15
        - Assignment for Week 15
        - 16 Multi-Factor Authentication (Mfa)
    - Ojt/Practicum 1
    - Social And Professional Issues
    - System Integration And Architecture 2
- Courses

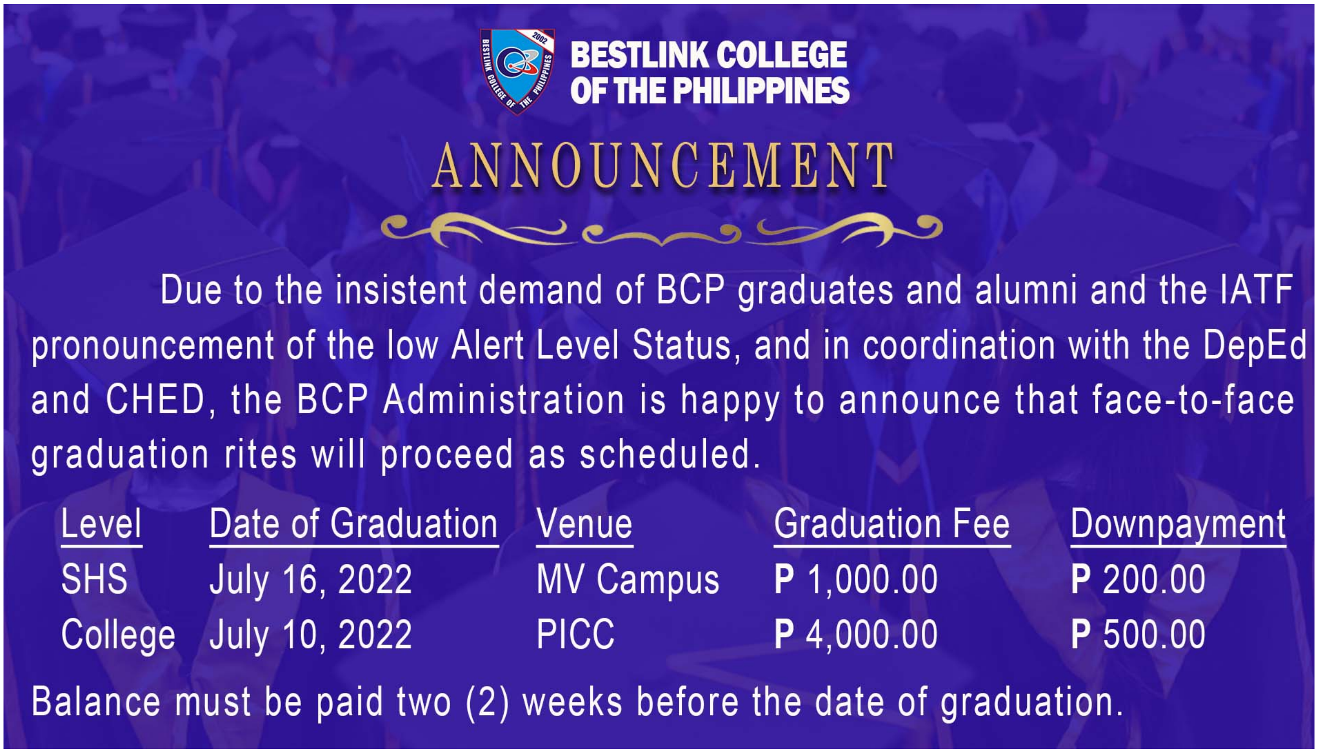
Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Graduation Announcement



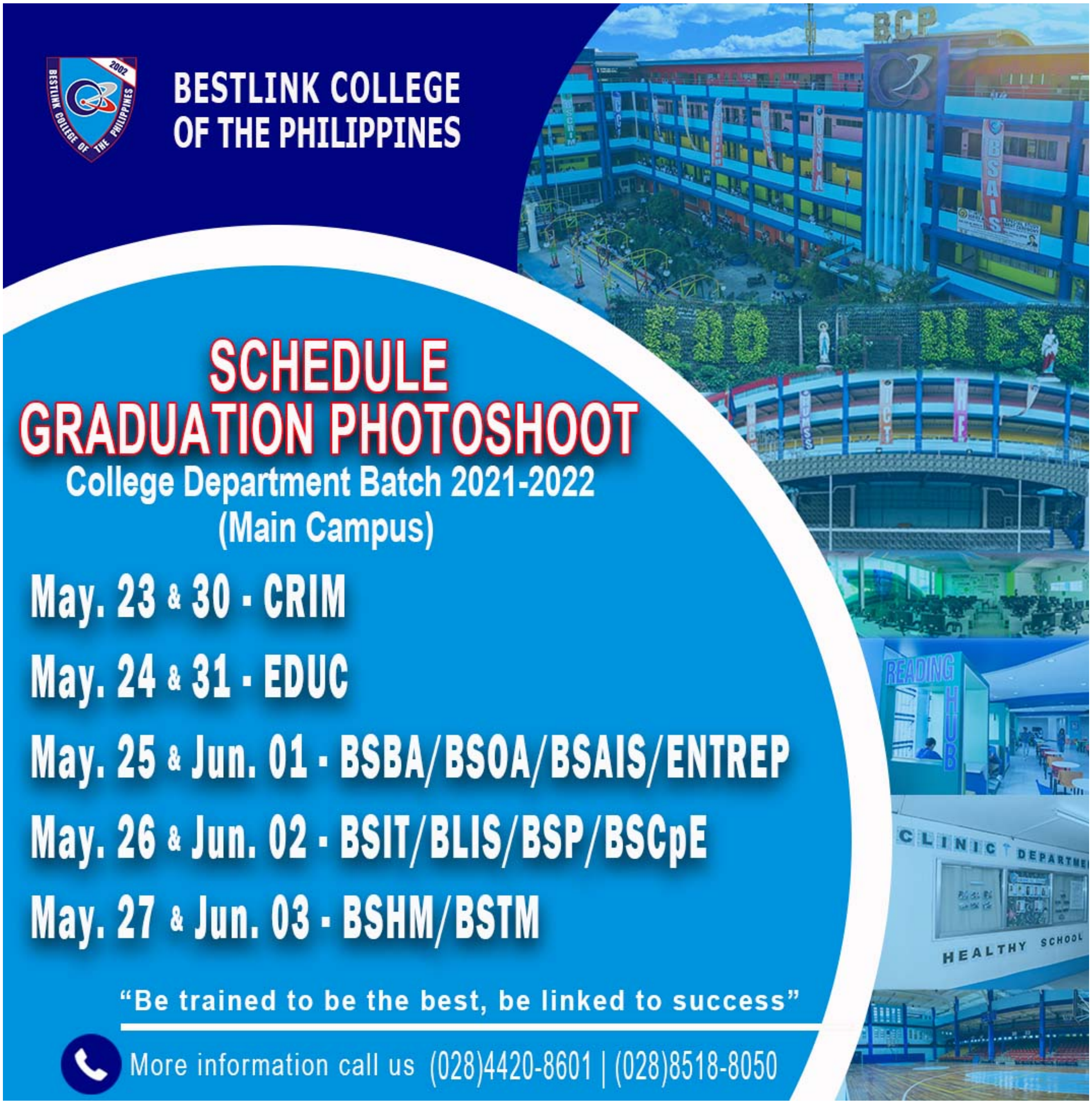
BESTLINK COLLEGE
OF THE PHILIPPINES

ANNOUNCEMENT

Due to the insistent demand of BCP graduates and alumni and the IATF pronouncement of the low Alert Level Status, and in coordination with the DepEd and CHED, the BCP Administration is happy to announce that face-to-face graduation rites will proceed as scheduled.

Level	Date of Graduation	Venue	Graduation Fee	Downpayment
SHS	July 16, 2022	MV Campus	**P** 1,000.00	**P** 200.00
College	July 10, 2022	PICC	**P** 4,000.00	**P** 500.00

Balance must be paid two (2) weeks before the date of graduation.



BESTLINK COLLEGE
OF THE PHILIPPINES

SCHEDULE GRADUATION PHOTOSHOOT

College Department Batch 2021-2022
(Main Campus)

May. 23 & 30 - CRIM

May. 24 & 31 - EDUC

May. 25 & Jun. 01 - BSBA/BSOA/BSAIS/ENTREP

May. 26 & Jun. 02 - BSIT/BLIS/BSP/BSCpE

May. 27 & Jun. 03 - BSHM/BSTM

"Be trained to be the best, be linked to success"

☎ More information call us (028)4420-8601 | (028)8518-8050

2002
BESTLINK COLLEGE OF THE PHILIPPINES
BCP
BSAIS
GOD BLESS
READING HUB
CLINIC DEPARTMENT
HEALTHY SCHOOL

BESTLINK COLLEGE OF THE PHILIPPINES

SCHEDULE GRADUATION PHOTOSHOOT

Bulacan Branch Batch 2021-2022

May 28

8am - 12nn: Senior High School

12nn - 5pm: College Department

"Be trained to be the best, be linked to success"

☎ More information call us (028)4420-8601 | (028)8518-8050

Activities

- Assignments
- Forums
- Quizzes
- Resources

Bestlink College of the Philippines
College Department