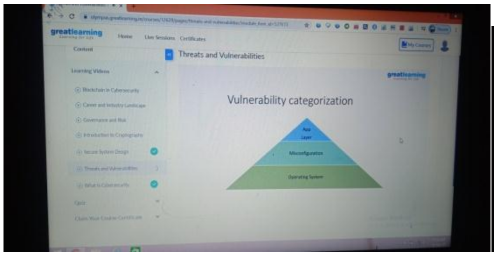
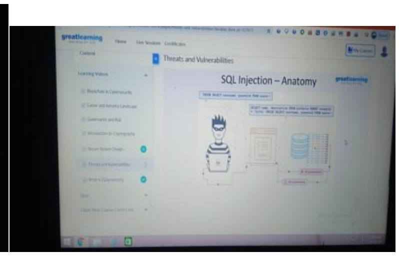
REPORT

Date:	17/06/2020	Name:	SAFIYA BANU
Course:	CYBER SECURITY	USN:	4AL16EC061
Topic:	➢ Vulnerabilities &PasswordSecurity ➢ What is Cryptography? ➢ Message integrity	Semester & Section:	8^{TH} B
Github Repository:	Safiya-Courses		

1. Vulnerabilities & Password Security





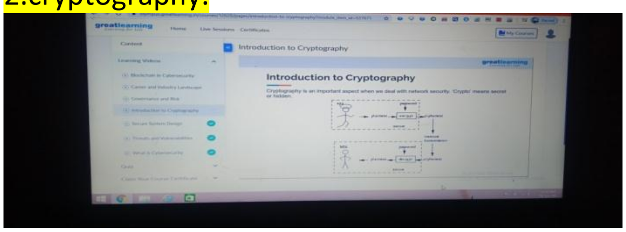
In computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, unauthorized actions within a computer system. To exploit a vulnerability, an attacker must have at least one tool or technique that can connect to a system weakness. In this frame, vulnerabilities are also known as the att Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulner This practice generally refers to software vulnerabilities in computing systems.

A security risk is often incorrectly classified as a vulnerability. The use of vulnerability with the same meaning lead to confusion. The risk is the potential of a significant impact resulting from the exploit of a vulnerability. The vulnerabilities without risk: for example when the affected asset has no value. A vulnerability with one or m instances of working and fully implemented attacks is classified as an exploitable vulnerability—a vulnerability f exploit exists. The window of vulnerability is the time from when the security hole was introduced or manifested software, to when access was removed, a security fix was available/deployed, or the attacker was disabled—s attack.

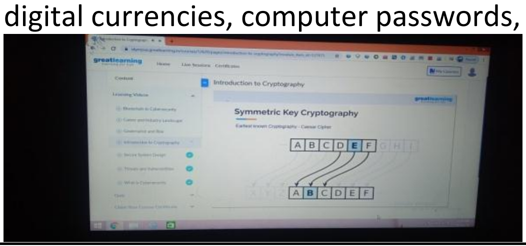
Security bug (security defect) is a narrower concept: there are vulnerabilities that are not related to software site, personnel vulnerabilities are examples of vulnerabilities that are not software security bugs.

Constructs in programming languages that are difficult to use properly can be a large source of vulnerabilities.yo security program. Equally, significant changes to your organisational structure may require another evaluatio strategy to ensure it meets your evolving business needs.

2.cryptography.



Cryptography, or cryptology (from Ancient Greek: κρυπτός, romanized: kryptós "hidden, secret"; and γράφειν gr write", or -λογία -logia, "study", respectively), is the practice and study of techniques for secure communica presence of third parties called adversaries. More generally, cryptography is about constructing and analyzin that prevent third parties or the public from reading private messages; various aspects in information security s confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptograph cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical e communication science, and physics. Applications of cryptography include electronic commerce, chip-based pay digital currencies, computer passwords, and military communications.

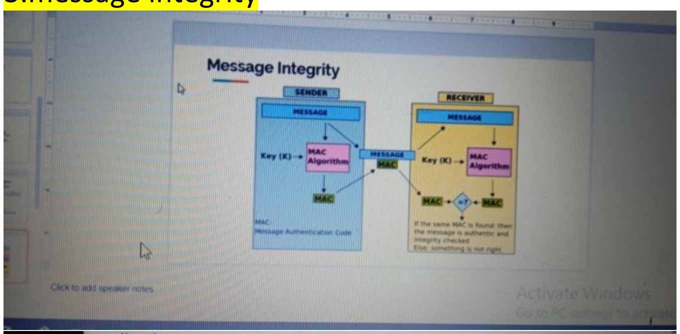


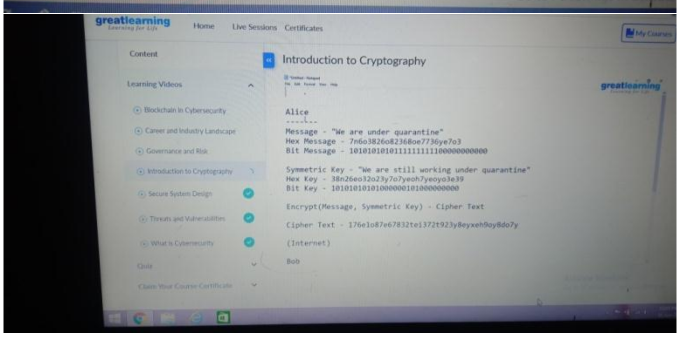
Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of informa
readable state to apparent nonsense. The originator of an encrypted message shares the decoding techniqu
intended recipients to preclude access from adversaries. The cryptography literature often uses the names Ali
the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary. Since the deve
rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out
have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic
are designed around computational hardness assumptions, making such algorithms hard to break in prac
adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known pract
These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements
factorization algorithms, and faster computing technology require these solutions to be continually adapted.
information-theoretically secure schemes that provably cannot be broken even with unlimited computing
example is the one-time pad—but these schemes are more difficult to use in practice than the best theoreticall
but computationally secure mechanisms.

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography
for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or ev
its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to
disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major ro
rights management and copyright infringement of digital media.

3.message integrity





In cryptography, a message authentication code (MAC), sometimes known as a tag, is a short piece of informat
authenticate a message—in other words, to confirm that the message came from the stated sender (its authe
has not been changed. The MAC value protects both a message's data integrity as well as its authenticity, l
verifiers (who also possess the secret key) to detect any changes to the message content.

Informally, a message authentication code system consists of three algorithms:

A key generation algorithm selects a key from the key space uniformly at random.

A signing algorithm efficiently returns a tag given the key and the message.

A verifying algorithm efficiently verifies the authenticity of the message given the key and the tag. That is, retur
when the message and tag are not tampered with or forged, and otherwise return rejected.
For a secure unforgeable message authentication code, it should be computationally infeasible to compute a
the given message without knowledge of the key, even if for the worst case, we assume the adversary can forg
any message except the given one.
Formally, a message authentication code (MAC) system is a triple of efficient Algorithms (G, S, V) satisfying:
G (key-generator) gives the key k on input 1n, where n is the security parameter.
S (signing) outputs a tag t on the key k and the input string x.
V (verifying) outputs accepted or rejected on inputs: the key k, the string x and the tag t.
S and V must satisfy the following:
Pr [k ← G(1n), V(k, x, S(k, x)) = accepted] = 1.
A MAC is unforgeable if for every efficient adversary A
Pr [k ← G(1n), (x, t) ← AS(k, ·)(1n), x ∉ Query(AS(k, ·), 1n), V(k, x, t) = accepted] < negl(n),
where AS(k, ·) denotes that A has access to the oracle S(k, ·), and Query(AS(k, ·), 1n) denotes the set of the q
made by A, which knows n. Clearly we require that any adversary cannot directly query the string x on S, since
valid tag can be easily obtained by that adversary.