Cryptography and Network Security

Security goals and attacks

The notes for the lesson “Security goals and attacks”: chapters 1.1 to 1.2, with their figures, worked examples, exam traps, quizzes and exam question bank, in one file.

2 chapters | Chapters 1.1 to 1.2

About these notes

These are the notes for the University free n easy video lesson **Security goals and attacks** on Cryptography and Network Security: chapters 1.1 to 1.2, with every figure, worked example, exam trap and quiz, and the long-answer exam questions on these chapters.

1.1 Security goals: confidentiality, integrity, availability (CIA)

Every security requirement you meet this year is one of three promises about data and service. Keep the data secret — confidentiality. Keep the data correct — integrity. Keep the service reachable — availability. A UPI payment shows all three at once: the amount must stay private, must not change in transit, and the bank's server must answer before the app times out. Engineers call these the CIA triad. Almost every exam question about a security incident is really asking which of the three broke.

Three promises about one message

Confidentiality means only allowed parties can read the data. A UPI payment leaves your phone carrying the payee address, the amount and an encrypted PIN block. On a shop's open Wi-Fi, a sniffer can read every field the app fails to encrypt. Confidentiality is the promise that it cannot.

Integrity means the data is exactly what the sender wrote. A mark sheet row says 18 out of 20 and someone edits it to 20. Nothing crashes, no error is shown, the record simply says something else. Integrity fails when a change happens and nobody detects it.

Availability means the service answers when a real user needs it. Tatkal opens at 10:00 and lakhs of people refresh the IRCTC page at that second; the site must still take bookings. Availability fails when the service is slow, down or unreachable.

A control usually protects one goal and costs another. The next chapter separates what you promise (a service) from the tool that delivers it (a mechanism).

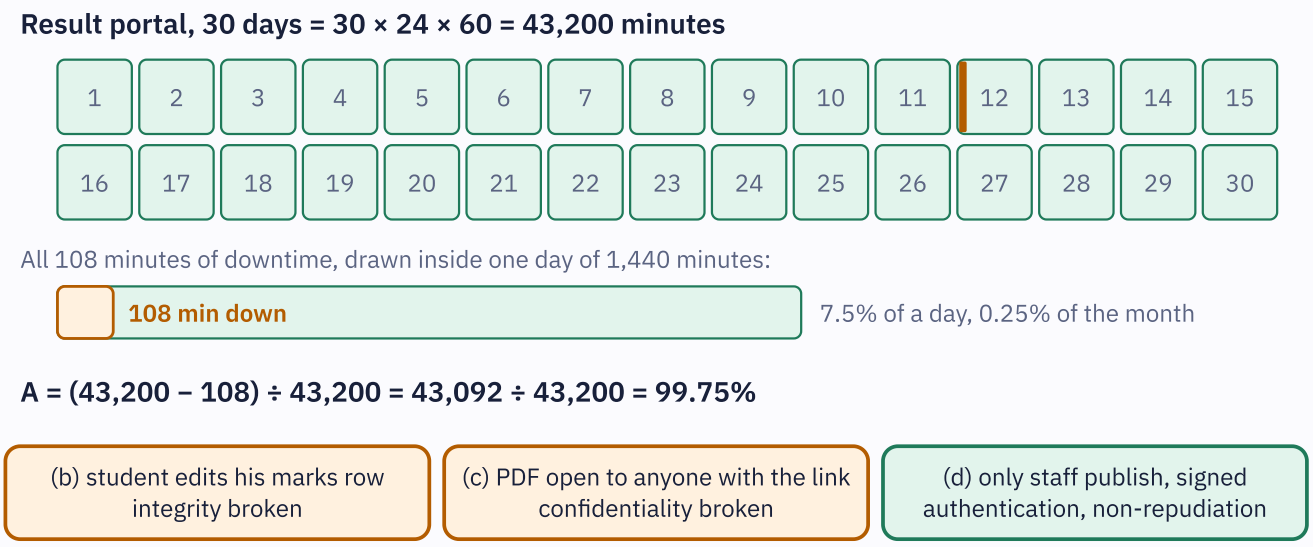


Figure 1.1.1 Over 30 days (43,200 minutes) the portal was down for 108 minutes, so its availability is 43,092 ÷ 43,200 = 99.75%. The other three events each touch one named goal.

The extra goals and the DAD set

Some syllabi list three more goals beside CIA.

- **Authentication**: each party proves who it is before the exchange. Your app verifies the bank's certificate; you prove yourself with a PIN.
- **Accountability**: every action is traceable to a named entity. The bank log shows which employee opened which account, and when.
- **Non-repudiation**: a party cannot later deny an action it really did. A digitally signed payment instruction cannot be waved away as 'I never sent that'.

The mirror image of CIA is the failure set some syllabi call **DAD**: *disclosure* breaks confidentiality, *alteration* breaks integrity, *destruction* (or denial) breaks availability. Describe an attack by the goal it breaks and the marking becomes easy.

Controls trade off, and trust must be stated

Controls compete for the same resources. Encrypting every field of a payment request protects confidentiality, but CPU cost per request rises, queues grow, and at peak the service slows — availability drops. Locking an account after three wrong PINs stops guessing, but an attacker who knows your username can lock you out on purpose. Security is a balance, not a maximum.

The balance is written down as a trust and threat model. It answers four questions.

1. Who is trusted: users, admins, the cloud provider, the certificate authority.
2. What each trusted party can do: read a row, sign a certificate, restart a server.
3. What you assume they will not do: steal data, collude, or make careless mistakes.
4. What happens when an assumption is false: a lost admin laptop counts as a disclosure event.

Confidentiality matrix and uptime as a number

A **confidentiality determination matrix** lists assets against data classes and records who may read each one. Build it before choosing controls: a Restricted row needs encryption at rest, a Public row does not. Keep it short, one line per asset.

ASSET	CLASS	MAY BE READ BY
Published result PDF	Public	Anyone with the link
Internal marks sheet	Internal	Exam-cell staff
Question paper before the exam	Restricted	Paper setters and controller
Student database dump	Restricted	Database admins only

Availability is quoted as a percentage over a stated period, never as the sentence 'the server is up'.

A = (T − D) ÷ T × 100

A is availability in percent; T is the total minutes in the stated period (days × 24 × 60); D is the minutes the service was unusable.

WORKED EXAMPLE

Question. A college result portal must run continuously for 30 days. (a) It was unusable for 108 minutes. Compute its availability. (b) A student edits his own marks row directly in the database. (c) A mark sheet PDF is readable by anyone holding the link, with no login. (d) Only exam-cell staff can publish results, and each publish is digitally signed. Name the goal broken or provided in (b), (c) and (d).

1. (a) Total minutes in the stated period: T = 30 days × 24 hours × 60 minutes = 43200 minutes.
2. Usable minutes: T − D = 43200 − 108 = 43092 minutes.
3. Availability: A = 43092 ÷ 43200 = 0.9975.
4. In percent: A = 0.9975 × 100 = 99.75%.
5. (b) The record changed and nobody detected it: integrity is broken.
6. (c) Data is readable by people who were never authorised: confidentiality is broken.
7. (d) Staff identity is proved, and a signature stops later denial: authentication and non-repudiation are provided.

Output

```
43200
43092
99.75
```

Answer. Availability is 99.75% over 30 days; (b) breaks integrity, (c) breaks confidentiality, and (d) provides authentication and non-repudiation.

EXAM TRAPS

- Writing 'security means confidentiality'. Marks come from naming the goal a stated incident broke: a crash is availability, a silent edit is integrity, a leak is confidentiality.
- Quoting availability as 'the server is up'. It is a percentage over a declared period, so always write the period and the down minutes.
- Assuming encryption gives integrity. It hides data from outsiders; a party who holds the key can still change it undetected. Detecting change needs a MAC or a signature (see a later lesson).
- Treating authentication and non-repudiation as one idea. A shared password authenticates but can be denied later; a digital signature cannot.
- Mismatching the DAD set. Disclosure pairs with confidentiality, alteration with integrity, destruction with availability — never cross them.

CHECK YOURSELF

– REMEMBER **Define the three goals of the CIA triad in one line each.** 2 marks

Confidentiality: only authorised parties can read the data. Integrity: the data is not changed undetected. Availability: the service is usable when an authorised user needs it.

– UNDERSTAND **A student changes his own marks row in the college database, and no outsider ever reads the table. Which goal fails, and why not confidentiality?** 3 marks

Integrity fails, because the stored value no longer matches what the examiner recorded and nothing detected the change. Confidentiality is untouched: no unauthorised party gained read access.

– APPLY **A booking server must run for 7 days and was unusable for 20 minutes. Compute availability in percent.** 3 marks

T = 7 × 24 × 60 = 10080 minutes. Usable = 10080 − 20 = 10060 minutes. A = 10060 ÷ 10080 × 100 = 99.80%.

– ANALYZE **A bank adds heavy field-level encryption to every login request. At peak load the login page takes 12 seconds instead of 3, and users give up. Which goal is being traded away, and against which benefit?** 4 marks

Availability is traded away: the service is technically up but too slow to use, so availability in the stated period falls. The benefit is confidentiality of the fields in transit. The fix is to encrypt selectively or add capacity, not to remove the control.

– APPLY **Classify these three assets in a confidentiality determination matrix and name the class for each: a published timetable PDF, an internal staff salary sheet, and the encryption keys of the exam server.** 3 marks

Timetable PDF: Public, anyone may read it. Salary sheet: Internal, staff and HR only. Encryption keys: Restricted, key custodians only.

– UNDERSTAND **Give the DAD failure that corresponds to each CIA goal.** 3 marks

Confidentiality — disclosure. Integrity — alteration. Availability — destruction (denial).

– ANALYZE **Only exam-cell staff may publish results, and each publish is digitally signed. Which two goals beyond CIA does this provide, and what does each one stop?** 4 marks

Authentication stops an outsider posing as staff, because identity is proved before publishing. Non-repudiation stops a staff member later denying that he published, because the signature is bound to him. Accountability follows if every publish is also logged with a name and time.

BEYOND THE SYLLABUS

Not for the exam. Industry writes the CIA triad into service contracts: a cloud provider's SLA states uptime as a percentage over a month with listed exclusions, and the shared-responsibility model splits the three goals between provider and customer. Regulators publish cyber-security frameworks that restate the same three promises as mandatory controls for banks and payment apps. Zero-trust architecture attacks the trust model itself, assuming the internal network is already hostile. Search next for zero trust, SLA uptime clauses, and confidentiality classification matrices.

1.2 Security attacks, services and mechanisms

A security course needs three words kept apart. An attack is an action that breaks something. A service is a promise the system makes to its users, such as "nobody else can read this". A mechanism is the tool that keeps that promise, such as encryption. The service and mechanism lists come from X.800, an ITU-T standard. The four attack classes come from the OSI attack taxonomy used in the standard security texts. Exam questions ask you to move between the three columns.

You need 1.1, because each service here protects one of the three goals defined there.

Passive and active attacks

Watch one message travel from sender to receiver and ask what an attacker can do. There are four answers.

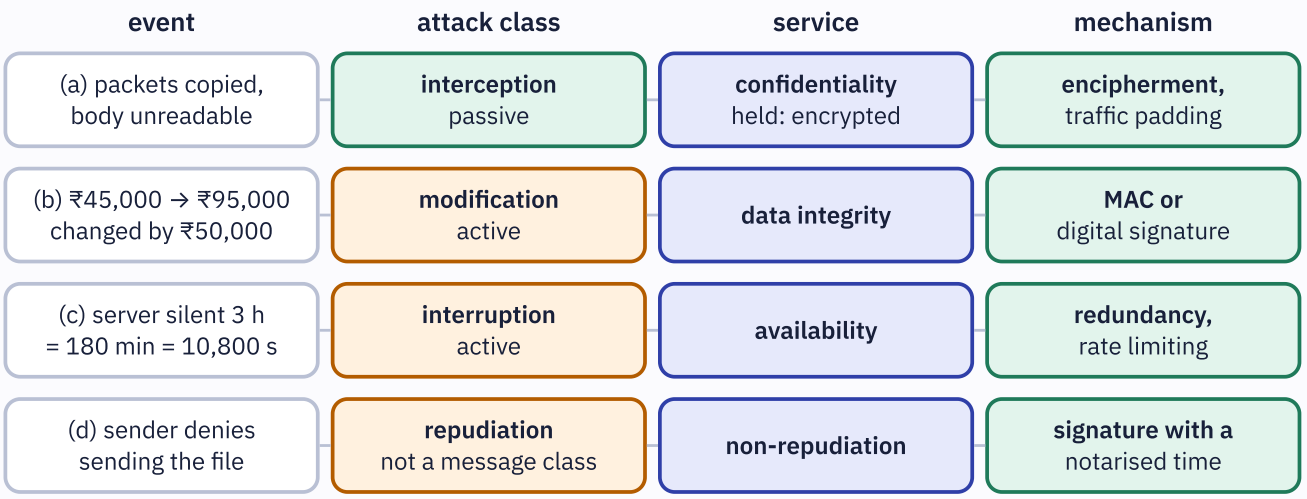
- **Interruption**: the message or the service is destroyed or blocked. Goal: availability.
- **Interception**: an unauthorised party reads the message. Goal: confidentiality.
- **Modification**: the message is changed before it arrives. Goal: integrity.
- **Fabrication**: a new message is inserted and made to look like it came from a real sender. Goals: integrity and authentication.

These four are the attack classes. Every named attack is one of them. A man-in-the-middle attack is interception plus modification. A flood that drowns a server is interruption.

A second cut is passive and active. A *passive* attack only observes. Two forms: release of message contents, and traffic analysis, which reads who talks to whom, when, and how many bytes, even when the bytes are scrambled. Nothing changes, so no checksum fails and detection is almost impossible. Defence is prevention: encryption, traffic padding, careful routing.

An *active* attack changes the data stream or the service: interruption, modification, fabrication, masquerade, replay. Something now looks wrong, so the aim is detection plus recovery. Only interception is purely passive; the other three classes are active.

Where does replay sit? The copying is passive interception; the re-insertion is active. Its class is contested. Most texts call it modification of the message stream, because an old message is put in place of the fresh one expected. Some list it as fabrication, because a copy is inserted. Either answer is accepted; say which you mean.



Read it backwards in the exam: start from the mechanism and name the service it protects.

Figure 1.2.1 Each event from the salary-file example in one row: what happened, the attack class, the service it attacks and the mechanism that meets it. The changed amount is ₹50,000 and the outage 10,800 seconds.

The six services

A security service is a guarantee the system gives its users. The standard list has six items, from X.800. A service says what is promised, never how it is done.

- **Authentication**: *peer entity* authentication proves who the other side is at the start of a connection. *Data origin* authentication proves which party created one message, with or without a connection.
- **Access control**: only the listed users, under the listed conditions, may use a resource.
- **Data confidentiality**: content is unreadable to others. Four forms: connection, connectionless, selective field, and traffic flow (the pattern and volume are hidden too).
- **Data integrity**: the data arrives exactly as sent, with no change, insertion, deletion or replay.
- **Non-repudiation**: a party cannot later deny a message. Two forms: proof of origin, and proof of delivery.
- **Availability**: the service answers when asked.

Two pairs are easy to confuse. Integrity is not confidentiality: a readable message can still be protected against tampering, and an unreadable one can still be tampered with. Non-repudiation is not authentication: authentication convinces the receiver at the time, while non-repudiation convinces a third party, such as a court, months later.

The eight mechanisms

A mechanism is the tool or procedure that delivers a service. The standard list has eight. Some syllabi call mechanisms *security controls* and split them into preventive, detective and corrective.

- **Encipherment**: turning plaintext into ciphertext. Delivers confidentiality, and supports integrity and authentication when a key is involved.
- **Digital signature**: data plus a private-key transformation that anyone can check. Delivers integrity, origin authentication and non-repudiation.
- **Access control mechanisms**: passwords, access lists, capabilities, roles.
- **Data integrity mechanisms**: a check value or sequence number attached to the data, so any change is visible.
- **Authentication exchange**: a message protocol, such as challenge and response, that tests a claim of identity.
- **Traffic padding**: extra bits or extra messages, so the real length and timing are hidden.
- **Routing control**: choosing trusted links and relays, or changing route when one is suspect.
- **Notarization**: a trusted third party records facts about a message, such as time, origin and delivery.

The mapping is many-to-many. Non-repudiation needs a signature plus a timestamp from a notary. One signature gives integrity, origin authentication and non-repudiation in one action.

ATTACK CLASS	GOAL AT RISK	SERVICE	TYPICAL MECHANISM
Interruption	Availability	Availability	Redundancy, rate limiting
Interception	Confidentiality	Confidentiality	Encipherment, traffic padding
Modification	Integrity	Data integrity	MAC, digital signature
Fabrication	Integrity, authentication	Authentication, non-repudiation	Digital signature, authentication exchange

WORKED EXAMPLE

Question. An employee downloads the salary file from the office server. For each event give the attack class (if any), the service attacked, and one mechanism that would have helped. Compute the change in rupees and the outage in minutes and seconds. (a) A switch mirror copies the packets, but the file body is unreadable. (b) The amount field changes in transit from ₹45,000 to ₹95,000. (c) The file server stops answering for 3 hours. (d) After the transfer the sender denies sending the file.

1. (a) The attacker only copies; nothing is altered. Attack class = interception, passive. The contents stayed safe because encipherment was already applied. What is still exposed is the pattern of who sent what to whom and when; traffic padding and careful routing reduce that.
2. (b) The value inside the message changed. Attack class = modification, active. Service attacked = data integrity. Mechanism = a MAC or a digital signature over the amount field.
3. (c) The service stopped. Attack class = interruption, active. Service attacked = availability. Mechanism = redundancy, plus rate limiting at the edge. No cipher helps here.
4. (d) The message was genuine, but the sender now refuses to admit it. This is not one of the four message classes; it is the X.800 threat of repudiation. The receiver cannot later prove the sender sent the file, so the missing service is non-repudiation, met by a digital signature with a notarised timestamp. If a class must be named, note only that a false denial by a party is treated as fabrication by the receiving side.
5. Arithmetic for the amount: 95,000 − 45,000 = ₹50,000 change.
6. Arithmetic for the outage: 3 hours × 60 = 180 minutes; 180 × 60 = 10,800 seconds.

Answer. The amount changed by ₹50,000 and the outage lasted 180 minutes (10,800 seconds). The events map to interception (encipherment already protected the contents), modification (MAC or signature), interruption (redundancy), and repudiation (non-repudiation service, digital signature with notarised timestamp).

EXAM TRAPS

- Mixing the three columns. Writing "encryption" when a service is asked for, or "confidentiality" when a mechanism is asked for, loses marks. Read what the question wants: what breaks, what is promised, or how it is done.
- Calling a replay passive. The copying is passive interception, but the re-insertion is active. Say "modification of the message stream, sometimes listed as fabrication".
- Treating authentication and non-repudiation as one service. Authentication convinces the receiver at the time; non-repudiation must convince a third party later.
- Assuming encryption covers all of confidentiality. Traffic analysis still works on an encrypted stream, so traffic-flow confidentiality needs padding and routing control as well.
- Writing "encryption" as the mechanism against a DoS attack. Availability is met by redundancy, rate limiting and routing control, not by secrecy.

CHECK YOURSELF

– REMEMBER **Name the four attack classes and the goal each one attacks.** 2 marks

Interruption attacks availability, interception attacks confidentiality, modification attacks integrity, fabrication attacks integrity and authentication.

– REMEMBER **List the five X.800 security services.** 2 marks

Authentication, access control, data confidentiality, data integrity, non-repudiation. Many texts add availability as a sixth.

– UNDERSTAND **Why is a passive attack hard to detect, and what does that mean for defence?** 3 marks

Nothing is altered, so no check fails and no trace is left in the data. Defence is prevention: encryption, traffic padding, routing control, rather than detection after the fact.

– UNDERSTAND **State the difference between peer entity authentication and data origin authentication.** 3 marks

Peer entity authentication runs at connection setup and proves who is at the other end for the life of the connection. Data origin authentication proves the source of a single message, works without a connection, and says nothing about timing or other messages.

– APPLY **A captured message "PAY ₹45,000" is re-sent three times next week. Classify the attack, name the service broken, and give two mechanisms that would stop it.** 4 marks

Active attack. Its class is contested: modification of the message stream, sometimes listed as fabrication (replay); either is accepted. Services broken: data integrity, and also authentication and non-repudiation. Mechanisms: a data integrity mechanism with timestamps or sequence numbers that rejects old messages, and a digital signature so the copy cannot pass as fresh.

– APPLY **A switch mirror copies an encrypted stream. The payload is safe, but the attacker still learns which client talks to the server and for how long. Name the attack sub-type, the service that is missing, and one mechanism for it.** 4 marks

Passive interception of the traffic pattern, i.e. traffic analysis. Service missing: traffic-flow confidentiality. Mechanism: traffic padding, with routing control as a second option.

– ANALYZE **It is claimed that one digital signature gives three services at once. Which three, and where does the mechanism fail?** 6 marks

Data integrity (any change breaks the check), data origin authentication (only the private-key holder can produce it), and non-repudiation (the holder cannot deny it). It gives no confidentiality, because anyone with the public key reads the message. It gives no availability, because an attacker can still block delivery. It also fails if the private key is stolen, since the thief can sign in the owner's name.

BEYOND THE SYLLABUS

Not for the exam. X.800 survives because auditors need a fixed checklist: a security architecture document is a table of services, the mechanism that delivers each, and the person who owns it. Modern threat modelling frameworks such as STRIDE are close cousins, with one letter for each of spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. Zero-trust designs keep the same services but move the mechanisms from the network edge to every request.

Key terms of this lesson

TERM	MEANING OR FORMULA	CHAPTER
Confidentiality	The promise that data is readable only by those allowed to read it; broken by interception or a leak.	1.1
Integrity	The promise that data has not been changed, deleted or forged by anyone not allowed to do so.	1.1
Availability	The promise that the service answers legitimate users when they ask; broken by flooding or destruction.	1.1
Non-repudiation	A sender cannot later deny a message; delivered by digital signatures and audit logs, not by secrecy alone.	1.1
Confidentiality determination matrix	A table listing each data item against each role or condition, marking who may read it.	1.1
Fabrication	An active attack in which the attacker inserts false data or a false identity into the system.	1.2
Digital signature	A cryptographic mechanism that binds a message to a key so any change is detectable and the signer cannot deny it.	1.2
Access control	The security service that decides, per request, whether this subject may perform this action on this object.	1.2

Exam question bank

Long-answer exam questions on these chapters, each with an outline of the points an examiner looks for. Answer one in full on paper before you read its outline.

Remember and understand

– UNDERSTAND **Define the three CIA security goals. For a UPI payment app, give one concrete failure of each goal and name the goal being lost.** 8 marks

Correct definition of confidentiality, integrity, availability; One realistic UPI example per goal (data leak, tampered amount, app down during festival rush); Correctly names which goal each failure breaks; Mentions that authentication supports all three but is not itself one of them.

– UNDERSTAND **Distinguish between a security attack, a security service and a security mechanism. Give one example of each and show how they link.** 8 marks

Attack = action that compromises security; service = guarantee offered to users; mechanism = tool or procedure that implements the service; Example attack: interception; example service: data confidentiality; example mechanism: encipherment; Clear statement that a mechanism counters an attack in order to deliver a service; One line on why confusing the terms leads to bad design.

– UNDERSTAND **Classify security attacks into passive and active categories with sub-types, and place interception, modification, fabrication and replay in the correct class.** 8 marks

Passive: eavesdropping/interception, traffic analysis — goal is information, no change to data; Active: masquerade, replay, modification of messages, denial of service, fabrication; Correct placement of each named attack; Note that passive attacks are hard to detect, active attacks are easier to detect but harder to prevent.

Apply

– APPLY **You are the security officer for an online examination portal at a mid-sized institute. Build a confidentiality determination matrix for five data items and three roles, and explain how you would use it during access-control reviews.** 13 marks

Table with data items as rows and roles as columns; Each cell marked readable or not, with a stated condition where needed; Justification of at least two non-obvious decisions (for example, invigilator access to question papers only after the exam starts); How the matrix becomes an access-control rule set and an audit checklist; Mention of what to do when a new role is created.

Analyze and evaluate

– ANALYZE **Compare the CIA triad with the DAD triad. During a live DDoS on a power utility's billing site, which goal fails first and which goal should the response team protect at the cost of the others? Justify.** 13 marks

Correct expansion of DAD: disclosure, alteration, destruction; Mapping of each DAD item to the CIA goal it breaks; Analysis showing availability fails first in a DDoS, while integrity and confidentiality remain intact; Argument for prioritising availability of the control system over billing, with a stated reason; Note that deliberately taking a service offline to preserve integrity is a valid trade-off.

Glossary (terms used in this lesson)

Accountability	Being able to tie every action to an identified subject, so misuse can be traced.
Asset	Anything of value to the organisation — data, a service, a device, or its reputation.
Authentication	Proving that a subject is who it claims to be, before any access is granted.
Control	Any safeguard — technical, procedural or physical — that reduces risk.
Encipherment	The mechanism of transforming data with a key so unauthorised readers get nothing useful.

Sources and further reading

Textbooks

- William Stallings, *Cryptography and Network Security: Principles and Practice*: Opening chapters on security services, mechanisms and attack classification; later chapter on malicious software.
- William Stallings, *Network Security Essentials: Applications and Standards*: Part on attacks, services and mechanisms, and the chapter on intruders and malicious code.
- Behrouz A. Forouzan, *Introduction to Cryptography and Network Security*: First part on security goals, attacks and the services-and-mechanisms model.
- Atul Kahate, *Cryptography and Network Security*: Introductory chapters on security attacks, services, mechanisms and malware.

Open web resources

Each link below was opened by the book script on 10 Nov 2026 and returned a page; the pages were not read line by line.

- CVE Program — official vulnerability identifier list: www.cve.org
- NIST National Vulnerability Database: nvd.nist.gov
- FIRST — Common Vulnerability Scoring System (CVSS): www.first.org/cvss
- MITRE ATT&CK knowledge base of adversary tactics and techniques: attack.mitre.org
- NIST Computer Security Resource Center: csrc.nist.gov
- OWASP Foundation — web application security guidance: owasp.org

Syllabus: the University free n easy universal syllabus, built from top universities' syllabi.

Built for the University free n easy YouTube channel from the universal syllabus of Cryptography and Network Security (Oct 2026). Written with top universities' syllabi and standard textbooks; check a formula against your prescribed book before an exam, and report mistakes on the channel.