Secrets and Risks

Week 2 Core Lecture

(COMP6441/COMP6841/LAWS3040/CRIM3040)

Rahat Masood @Term 2, 2025, UNSW Sydney

Agenda

- Admin Reminders
- Origins and Evolution of Security
- Historical Examples
- Secrets and CIA
- Codes and Classical Ciphers
- Risk (Likelihood & Impact)
- Risk Assessment & Mitigation
- Type 1/Type II Errors

Consent/Ethics

- Course content may include ideas that could cause harm or disruption if misused
- Students must follow the **Good Faith Policy** in all courses
  - Do not act in ways that disrepute the course, staff, students, school, university, or ICT profession
  - Be a good citizen in all academic and professional conduct
  - Policy details: sec.edu.au/good-faith-policy
- Maintain a high standard of professionalism
- Show respect for others and consider the impact of your actions

Admin Reminders

- Swapping between 6441 and 6841
- Due Dates:
  - Week 1 Portfolio: **Tuesday 10th June at 4:00pm** at OpenLearning
  - Week 2 Activities Released: **Friday 6th June at 9:00am** at OpenLearning
  - Project Proposal: **Monday 16th June at 4:00pm** with Week 2 Portfolio at OpenLearning
- Project
  - Finalise your project idea in discussion with your tutor and record it in your portfolio.

THURSDAY 26TH JUNE 2025

SECeduCon5

CHAMPIONING CYBER SECURITY AS A PROFESSION

REGISTER NOW
WITH EARLY BIRD DISCOUNT CODE

STUDENT_25

Commonwealth Bank

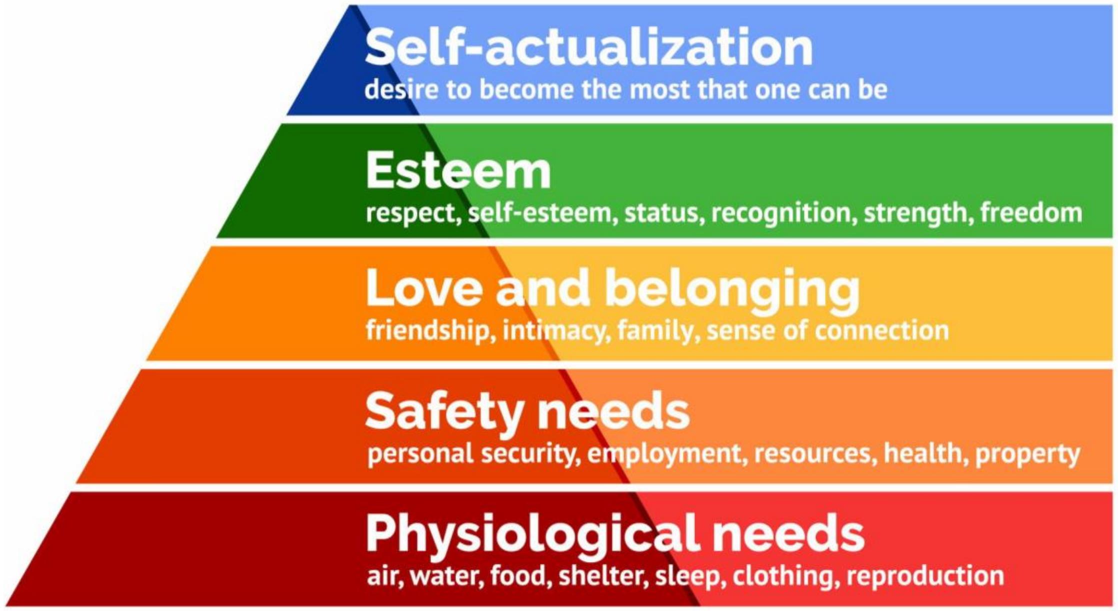
CYBER SECURITY
EDUCATION
AUSTRALIA

UNSW
SYDNEY

The Origins of Security – A Human Necessity

- Security in the History of Life
  - Security has always been central to survival i.e., from early humans to modern societies.
  - Rooted in Maslow's Hierarchy of Needs: Safety comes just after physiological needs.
  - Without a sense of safety, higher goals like love, esteem, and self-actualization are unattainable.

Remember from Week 1 Core Lecture

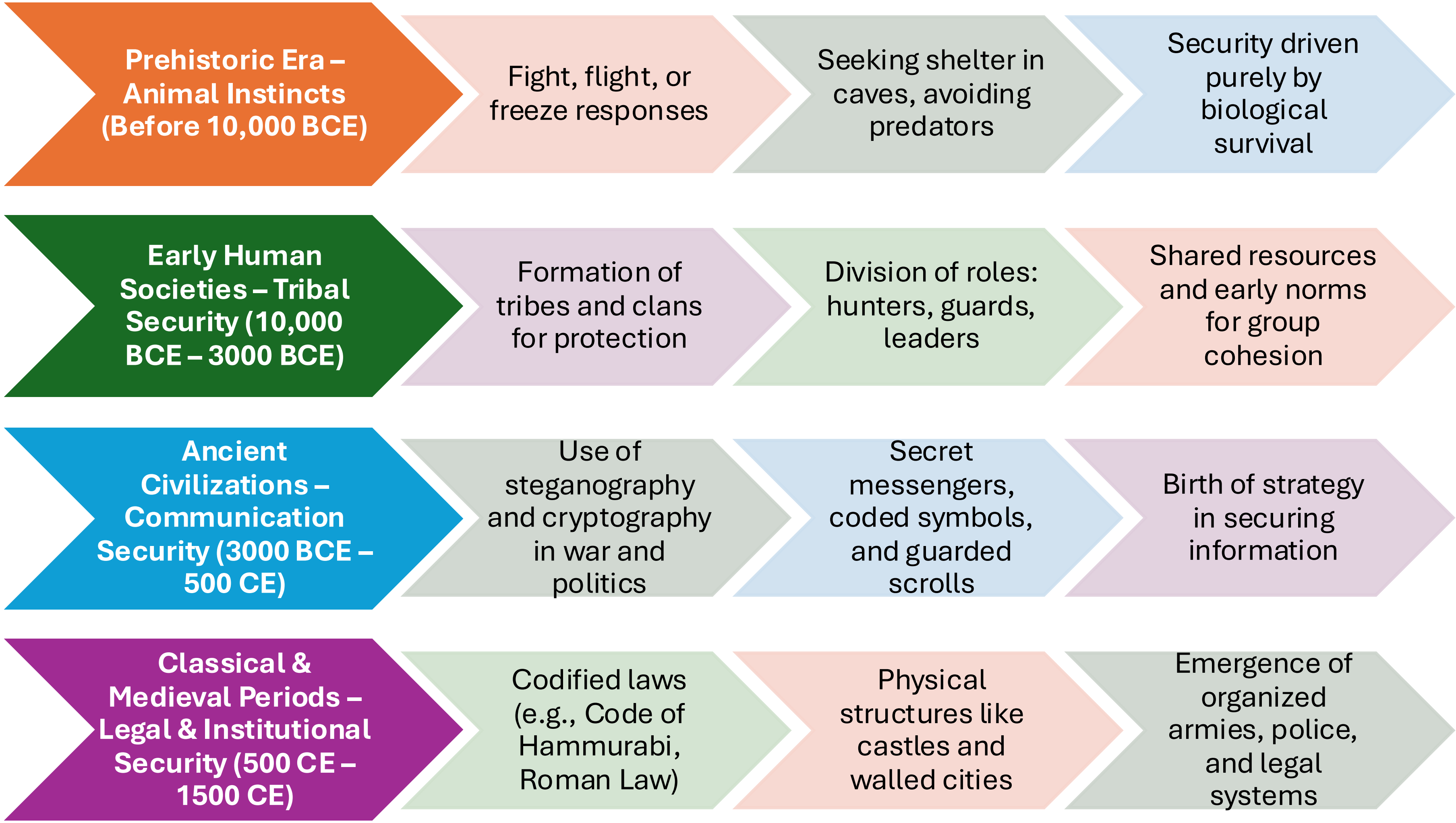


Self-actualization
desire to become the most that one can be
Esteem
respect, self-esteem, status, recognition, strength, freedom
Love and belonging
friendship, intimacy, family, sense of connection
Safety needs
personal security, employment, resources, health, property
Physiological needs
air, water, food, shelter, sleep, clothing, reproduction

The Evolution of Security

- From Survival to Systematic Protection
  - **Biological Security:** Instincts, hiding, forming groups
  - **Social Security:** Laws, rules, tribe protection
  - **Communication Security:** Protecting information became key to strategy and survival
  - Growing complexity required protection at multiple levels: physical, emotional, informational

The Evolution of Security



Prehistoric Era – Animal Instincts (Before 10,000 BCE)
- Fight, flight, or freeze responses
- Seeking shelter in caves, avoiding predators
- Security driven purely by biological survival

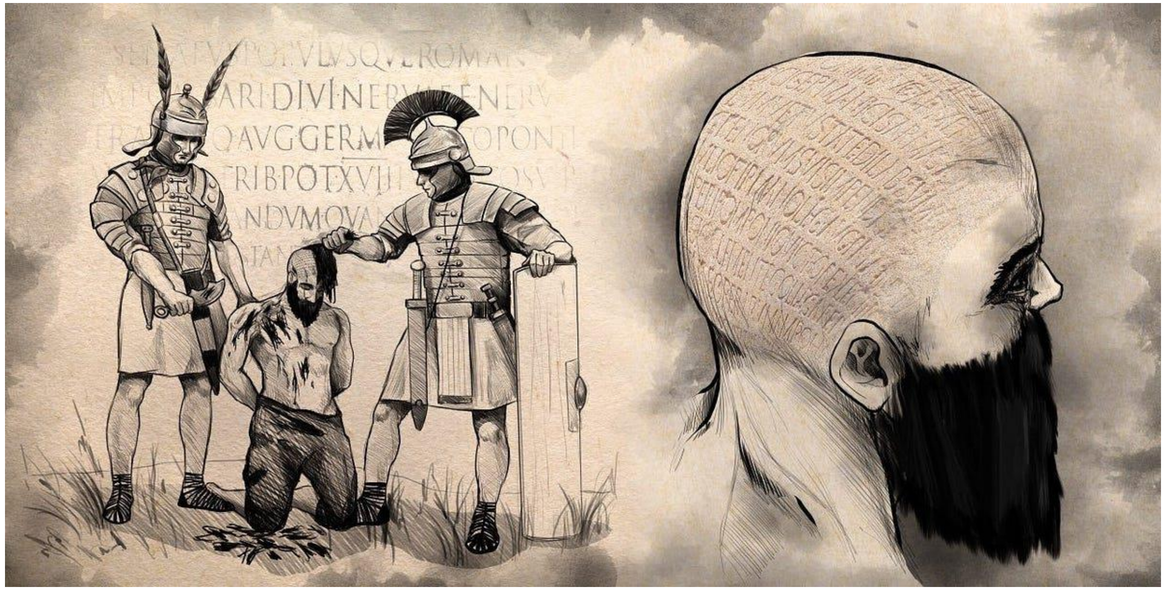
Early Human Societies – Tribal Security (10,000 BCE – 3000 BCE)
- Formation of tribes and clans for protection
- Division of roles: hunters, guards, leaders
- Shared resources and early norms for group cohesion

Ancient Civilizations – Communication Security (3000 BCE – 500 CE)
- Use of steganography and cryptography in war and politics
- Secret messengers, coded symbols, and guarded scrolls
- Birth of strategy in securing information

Classical & Medieval Periods – Legal & Institutional Security (500 CE – 1500 CE)
- Codified laws (e.g., Code of Hammurabi, Roman Law)
- Physical structures like castles and walled cities
- Emergence of organized armies, police, and legal systems

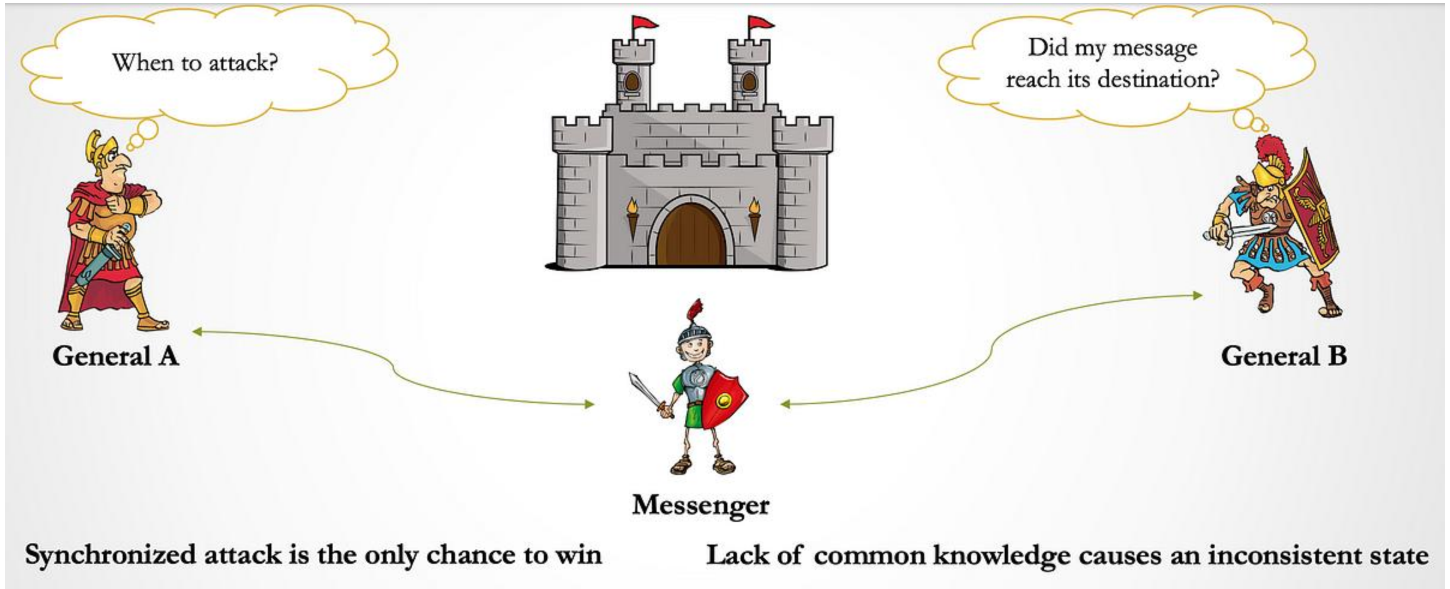
Historical Examples of Security in Practice

- Innovations in Early Security
  - **Steganography:** Ancient Greeks engraved messages on shaved heads, regrew hair



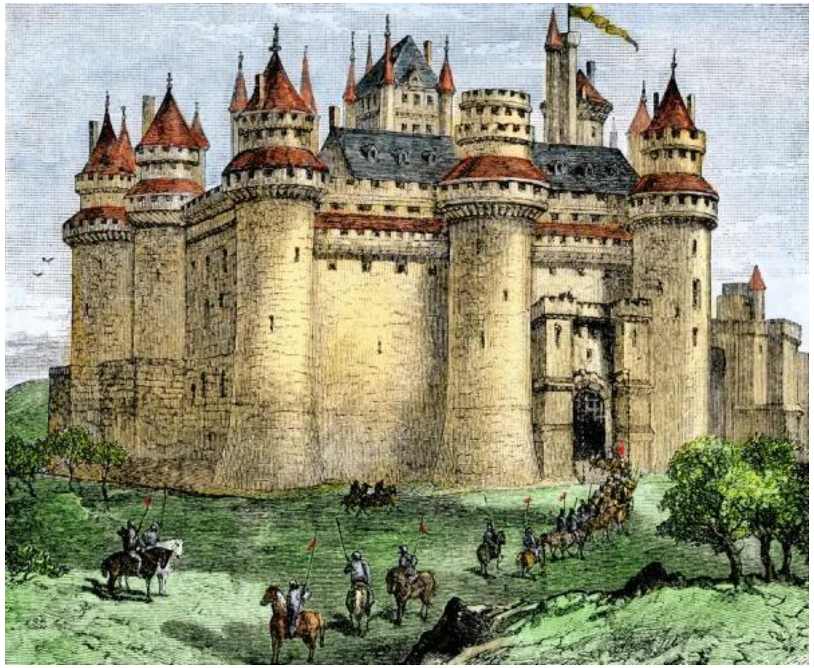
Historical Examples of Security in Practice

- Innovations in Early Security
  - **The Two Generals' Problem:** A classic thought experiment on the difficulty of secure coordination over unreliable communication


When to attack?
Did my message reach its destination?
General A
General B
Messenger
Synchronized attack is the only chance to win
Lack of common knowledge causes an inconsistent state

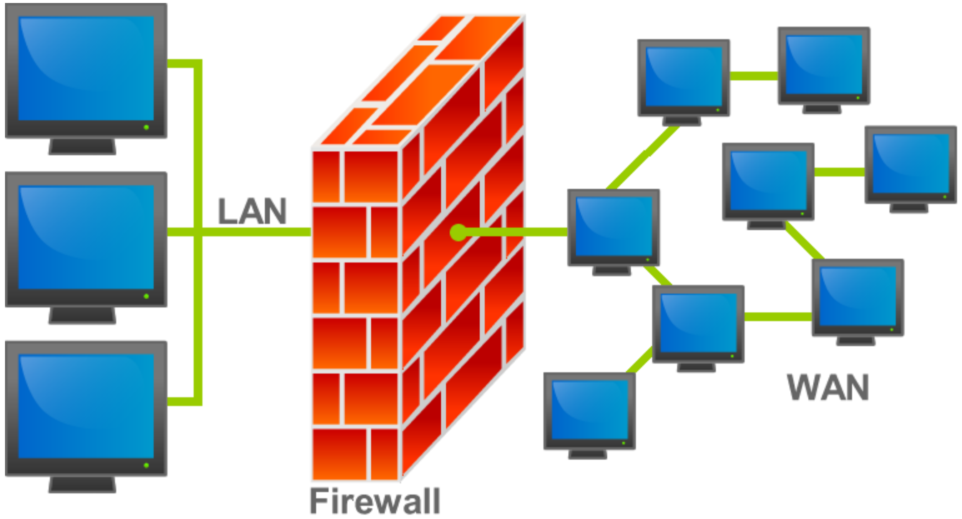
Historical Examples of Security in Practice

- Innovations in Early Security
  - **Castles & Fortresses:** Symbols of physical security – walls, moats, guards



The Importance of Security Today

- The Unchanging Need for Security
  - Security still forms the backbone of stable societies
  - Expanded domains: Cybersecurity, Data Privacy, National Security
  - As threats evolve, so must our approaches



Who Are We Defending Against?

There are many different motivations behind cyber criminals:

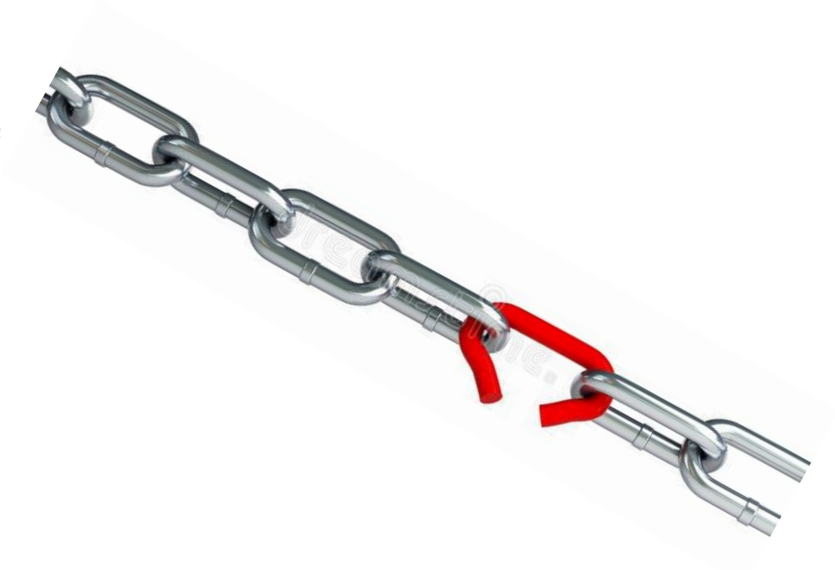
Actor	**Motivation**	**Example Tactics**
Cybercriminals	Financial gain	Phishing, ransomware, fraud
Hacktivists	Political or social agenda	Website defacement, DDoS
Nation-State Actors	Espionage, disruption	APTs, malware, cyberwarfare
Insiders	Revenge, negligence, or profit	Data theft, sabotage, accidental leak
Script Kiddies	Fun, bragging rights	Use of pre-made tools, website defacing
Competitors	Business advantage	Corporate espionage

What is a Secret?

- A secret is information deliberately kept hidden from others to protect its value or meaning.
- Why we keep secrets:
  - To protect privacy
  - To maintain advantage (e.g., military, business, games)
  - For trust, safety, or control
- Being given a secret:
  - Means trust, but also responsibility
  - You are now "on the inside"

How Do We Keep Secrets?

- Methods of protection:
  - Encryption: scrambling information
  - Physical security: safes, locked drawers
  - Behavioral secrecy: not telling, misdirection
- Everyone who knows = a risk:
  - Each individual becomes a potential point of failure
  - The more people know, the more likely a leak



The Properties of Secret (CIA Triad)

- The CIA Triad, a foundational security model:

  - Confidentiality

  ○ Ensuring that information is only accessible to those authorised to see it.

  - Integrity

  ○ Ensuring data is accurate and hasn't been tampered with.

  - Authentication (emphasised in this course over Availability)

  ○ Verifying the identity of users or systems before granting access.

In this course, **Authentication > Availability**, reflecting modern priorities where **identity verification** is a more pressing concern than uptime in many contexts.

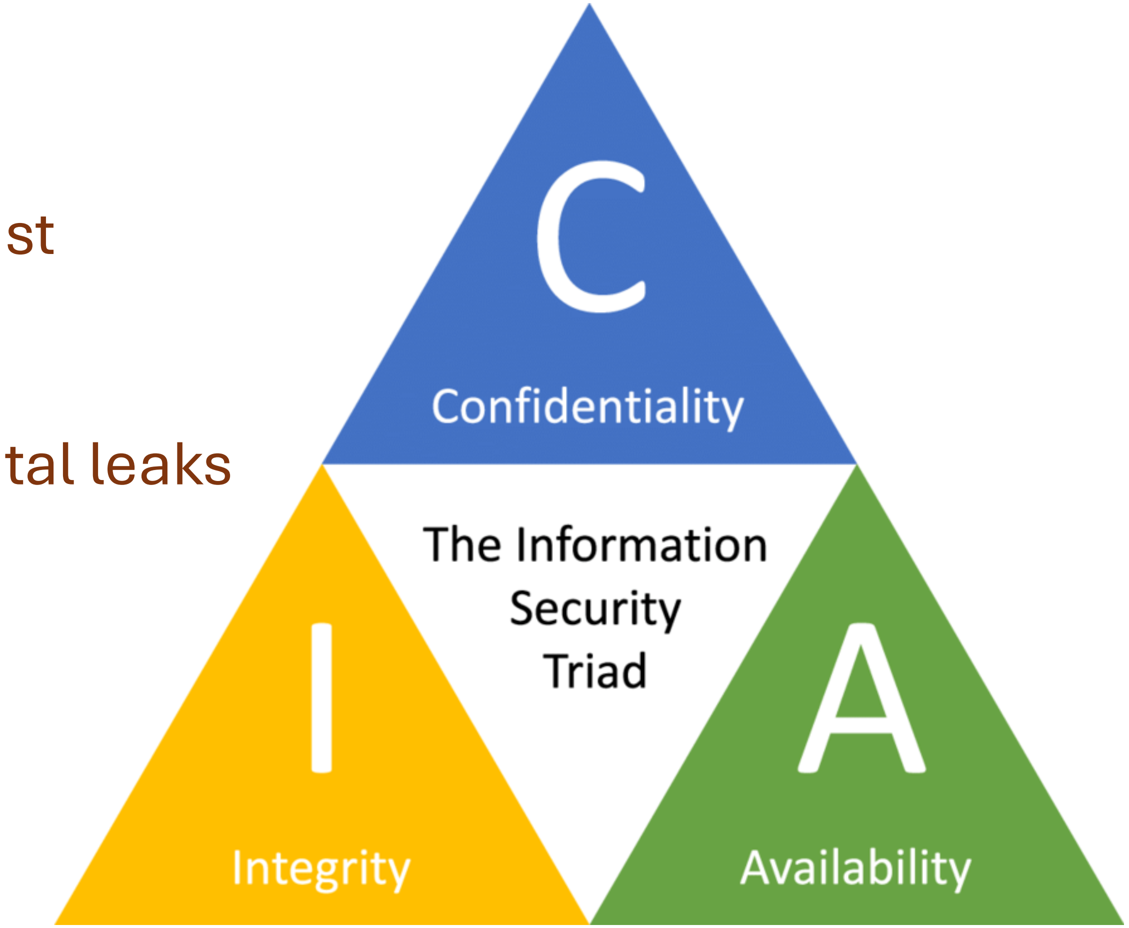
CIA Triad

Strengths:

- Strong encryption, limited access, high trust

Weaknesses:

- Human error, social engineering, accidental leaks



Beyond CIA: CIANA

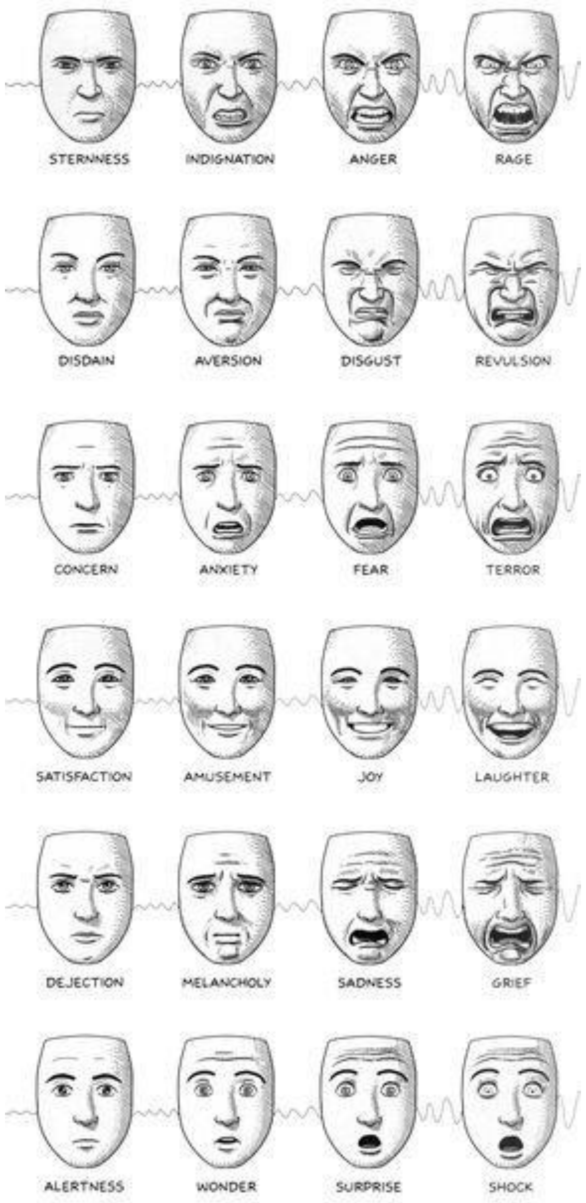
- Some security experts prefer CIANA, which includes:
  - **Confidentiality:** Ensuring information is accessible only to those authorized.
  - **Integrity:** Maintaining the accuracy and completeness of data.
  - **Authentication:** Verifying the identity of users and systems.
  - **Non-repudiation:** Guaranteeing that a sender cannot deny the authenticity of their signature on a document or a message they originated.
  - **Availability:** Ensuring that authorized users have reliable and timely access to systems and data when they need them.

Remember: Keeping Secrets Means Strong CIANA.
A failure in any one area can lead to a <u>leak, breach, or misuse of the secret.</u>

How Secrets Leak: ”Tells” and “Patterns”

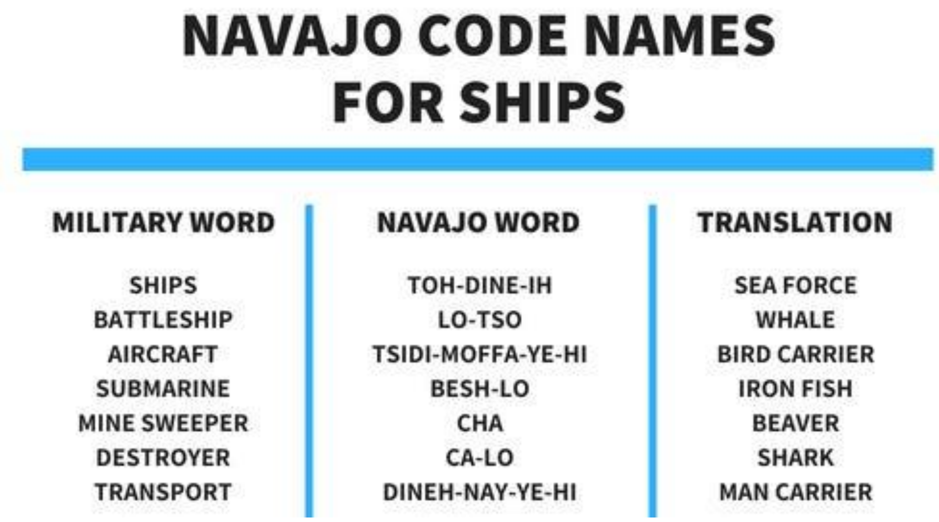
- “Tells” from Poker Theory:
  - Unintentional leakage through
  - Small, unconscious behaviours that hint at the truth
- Secrets often leak through body language or habits
- Patterns as Hints:

- Repeating actions or signals can create predictable behaviours
- Attackers look for patterns to infer secrets (e.g., typing rhythm, access times)



What is a Code?

- A code replaces words or phrases with other words, numbers, or symbols to convey meaning.
- **Example:**
  - “The package is delivered” = “The eagle has landed”
  - WWII Navajo Code Talkers used language as a secret code.
- **Used for:**
  - Hiding meaning in communication
  - Often context-specific (requires shared keybook or agreement)

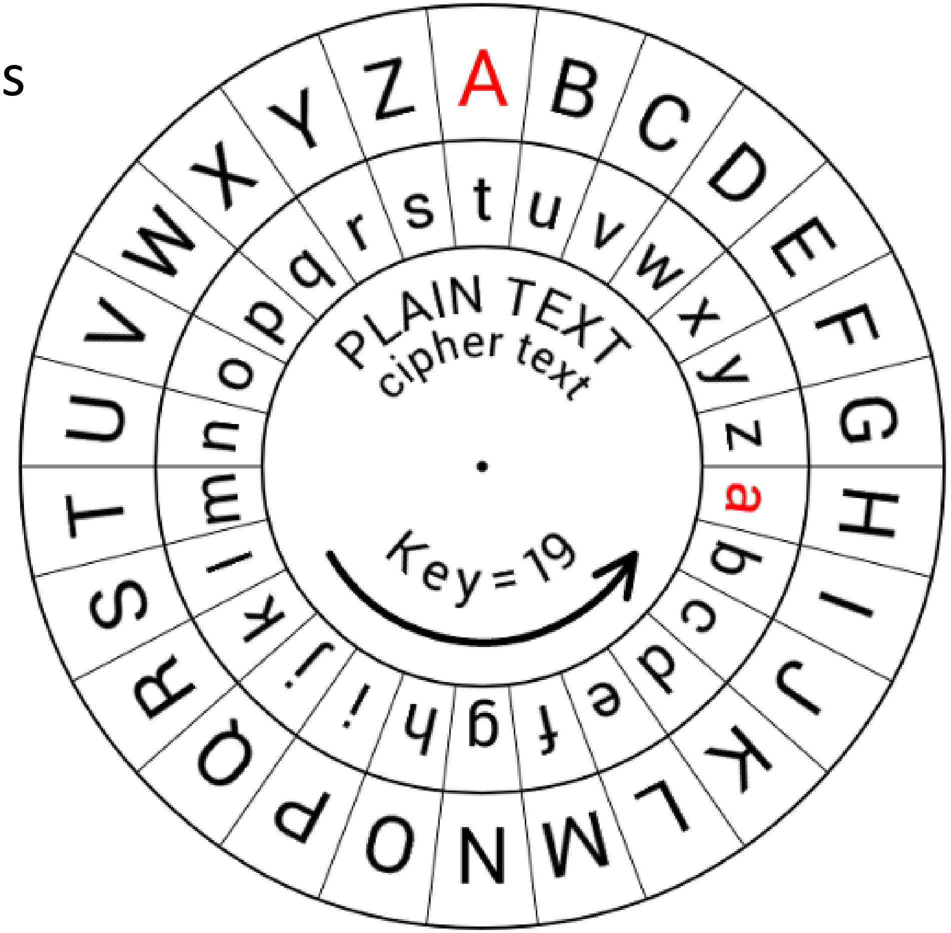


NAVAJO CODE NAMES FOR SHIPS

MILITARY WORD	NAVAJO WORD	TRANSLATION
SHIPS	TOH-DINE-IH	SEA FORCE
BATTLESHIP	LO-TSO	WHALE
AIRCRAFT	TSIDI-MOFFA-YE-HI	BIRD CARRIER
SUBMARINE	BESH-LO	IRON FISH
MINE SWEEPER	CHA	BEAVER
DESTROYER	CA-LO	SHARK
TRANSPORT	DINEH-NAY-YE-HI	MAN CARRIER

What is a Cipher?

- A cipher is a method of transforming individual letters or bits using a mathematical algorithm.
- **Example:**
  - Caesar Cipher: shift letters (A → D, B → E, etc.)
  - Modern: AES (Advanced Encryption Standard)
- **Used for:**
  - Cryptographic security (mathematical secrecy)
  - Digital communication (email, websites)


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
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
PLAIN TEXT
cipher text
Key = 19

Codes vs. Ciphers – What’s the Difference?

Aspect	**Code**	**Cipher**
Unit of change	Whole words/phrases	Individual letters, numbers, bits
Method	Symbolic replacement	Algorithmic transformation
Example	"Sunset" → "Alpha Bravo"	"HELLO" → "KHOOR" (Caesar Cipher)
Use case	Espionage, secret language	Cryptography, digital encryption

Key takeaway:

- Codes = substitute meaning
- Ciphers = scramble structure

History of Codes

- Steganography

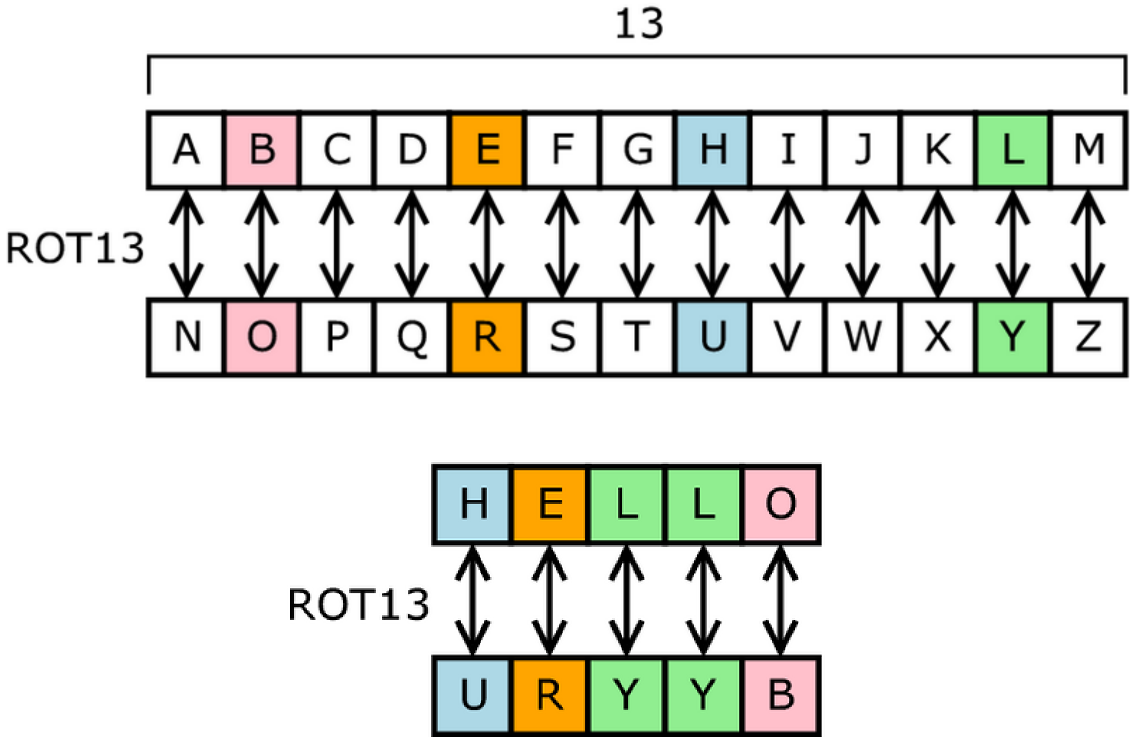
  - Six Design principles for military ciphers (Auguste Kerckhoffs 1883)
- Codes
- Classical Ciphers
- Simple Permutation + Substitution Ciphers
- Vignere
- Playfair

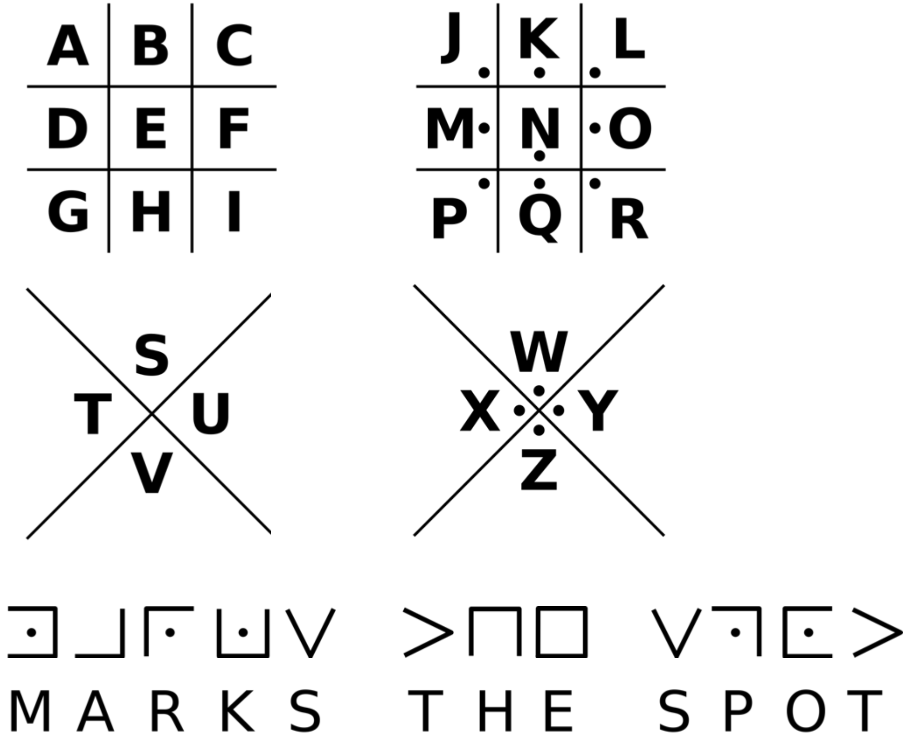
Cipher Design Becomes a Science (Kerckhoffs' Principles – 1883)

- Auguste Kerckhoffs' Six Principles for Military Ciphers (1883):
  - System must be practically indecipherable
  - No secrecy of the system, only of the key
  - Key must be easily changeable
  - Ciphertext must be transmissible via telegraph
  - Portable and operable without complex tools
  - Must be usable by people with limited training
- Key Insight:
  - Modern cryptography is built on these foundations
  - Emphasis on security through key secrecy, not algorithm secrecy

Classical Ciphers – The Building Blocks

- **Substitution Ciphers:**
  - Replace each letter with another (e.g., Caesar Cipher, ROT13, Pigeon Cipher)





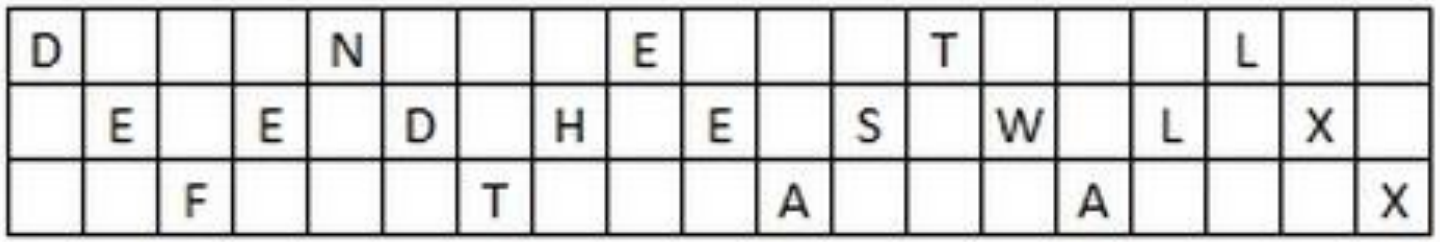
Classical Ciphers – The Building Blocks

- **Permutation (Transposition) Ciphers:**
  - Rearrange letters of the message (e.g., Rail Fence Cipher, Columnar Cipher)

Rail Fence Cipher

Plaintext: *defend the east wall*

Key: 3



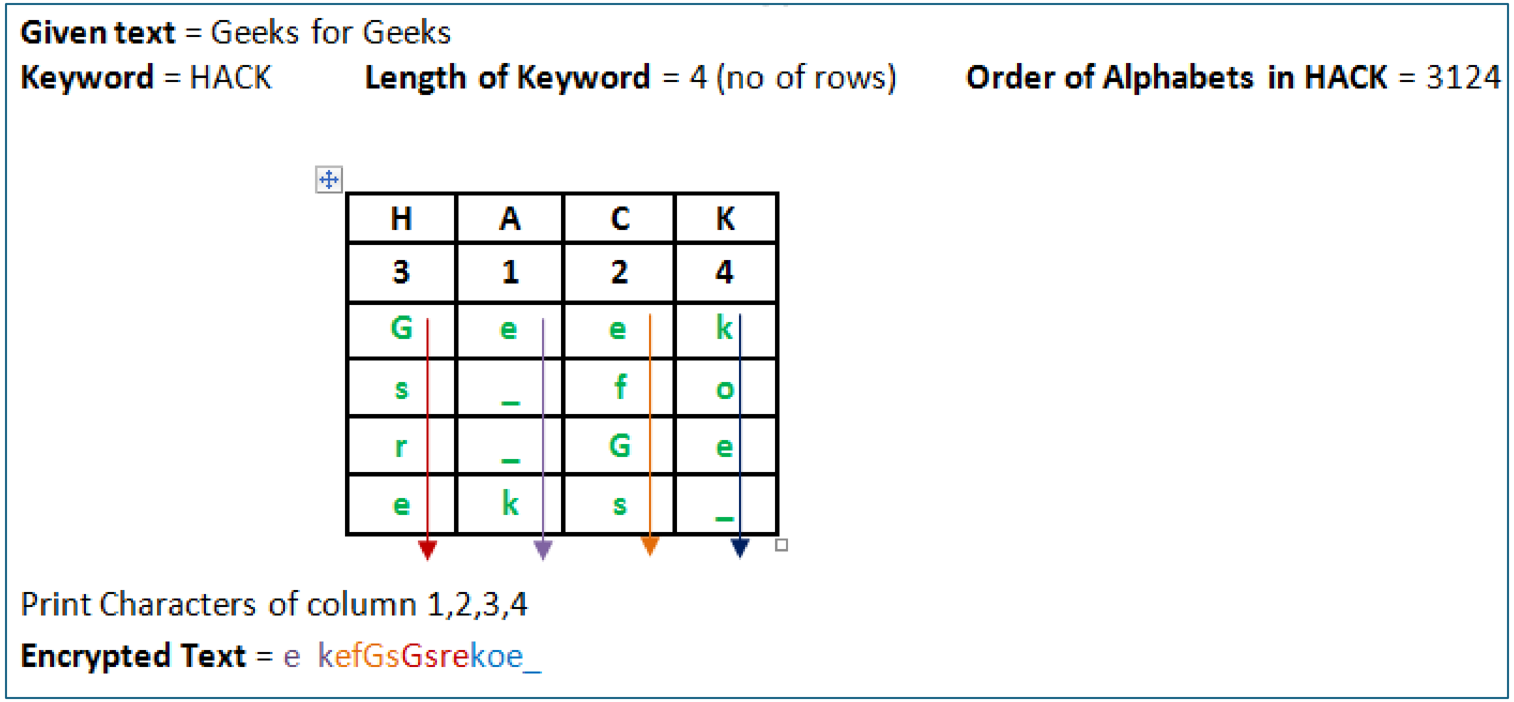
D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

Ciphertext: DNETLEEDHESWLXFTAAX

Classical Ciphers – The Building Blocks

- **Permutation (Transposition) Ciphers:**
  - Rearrange letters of the message (e.g., Rail Fence Cipher, Columnar Cipher)

Columnar Cipher



Given text = Geeks for Geeks

Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4

Encrypted Text = e kefGsGsrekoe_

Classical Ciphers – The Building Blocks

- **Combined Approaches:**
  - Many classical ciphers used both substitution + permutation for stronger protection

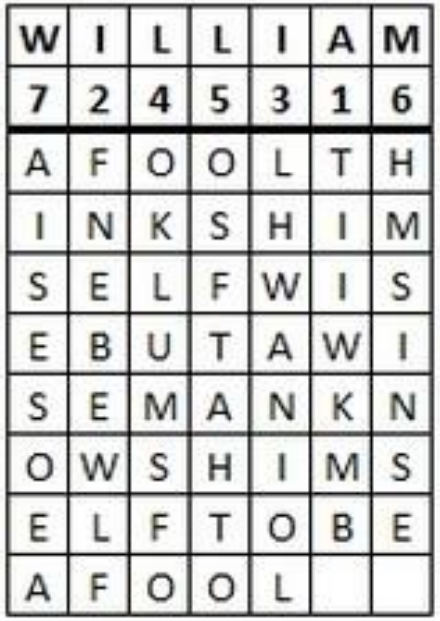
Step 1:

Plaintext: *“a fool thinks himself wise, but a wise man knows himself to be a fool”*

Key: WILLIAM

Cipher Method: Columnar Transposition

Ciphertext 1: TIIWK MBFNE BEWLF LHWAN IOLOK LUMSF OOSFT AHTOH MSINS EAISE SOEA



W	I	L	L	I	A	M
7	2	4	5	3	1	6
A	F	O	O	L	T	H
I	N	K	S	H	I	M
S	E	L	F	W	I	S
E	B	U	T	A	W	I
S	E	M	A	N	K	N
O	W	S	H	I	M	S
E	L	F	T	O	B	E
A	F	O	O	L		

Classical Ciphers – The Building Blocks

- **Combined Approaches:**
  - Many classical ciphers used both substitution + permutation for stronger protection

Step 2:

Cipher Method: Ceaser Cipher

Key: backward by 6

Ciphertext 1: TIIWK MBFNE BEWLF LHWAN IOLOK LUMSF OOSFT AHTOH MSINS EAISE SOEA

T → N	M → G	B → V	L → F	I → C	L → F	O → I	A → U	M → G	E → Y	S → M
I → C	B → V	E → Y	H → B	O → I	U → O	O → I	H → B	S → M	A → U	O → I
I → C	F → Z	W → Q	W → Q	L → F	M → G	S → M	T → N	I → C	I → C	E → Y
W → Q	N → H	L → F	A → U	O → I	S → M	F → Z	O → I	N → H	S → M	A → U
K → E	E → Y	F → Z	N → H	K → E	F → Z	T → N	H → B	S → M	E → Y	

Ciphertext 2: NCCQE GVZHY VYQFZ FBQUH CIFIE FOGMZ IIMZN UBNIB GMCHM YUCMY MIYU

What is Risk?

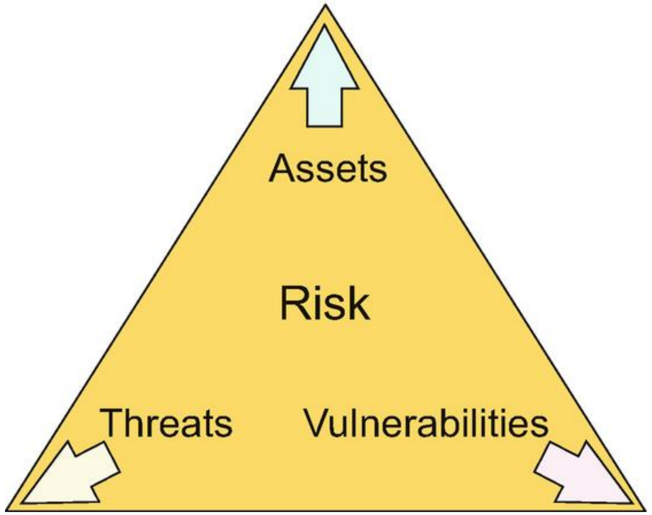
- When we discuss secrets or security more broadly, we must ask:

“What is the risk of this being exposed, stolen, or misused?”

- Risk is the potential for loss or damage when a threat exploits a vulnerability.

Risk = Likelihood × Impact

- **Why it matters:**
  - Helps prioritize threats – not all risks are equal
  - Guides decision-making in security, business, and planning



Likelihood vs Impact

Term	Definition	Example
Likelihood	How probable it is that a risk will occur	“How likely is a cyberattack?”
Impact	How severe the damage would be if it happens	“Would it cause downtime, data loss?”

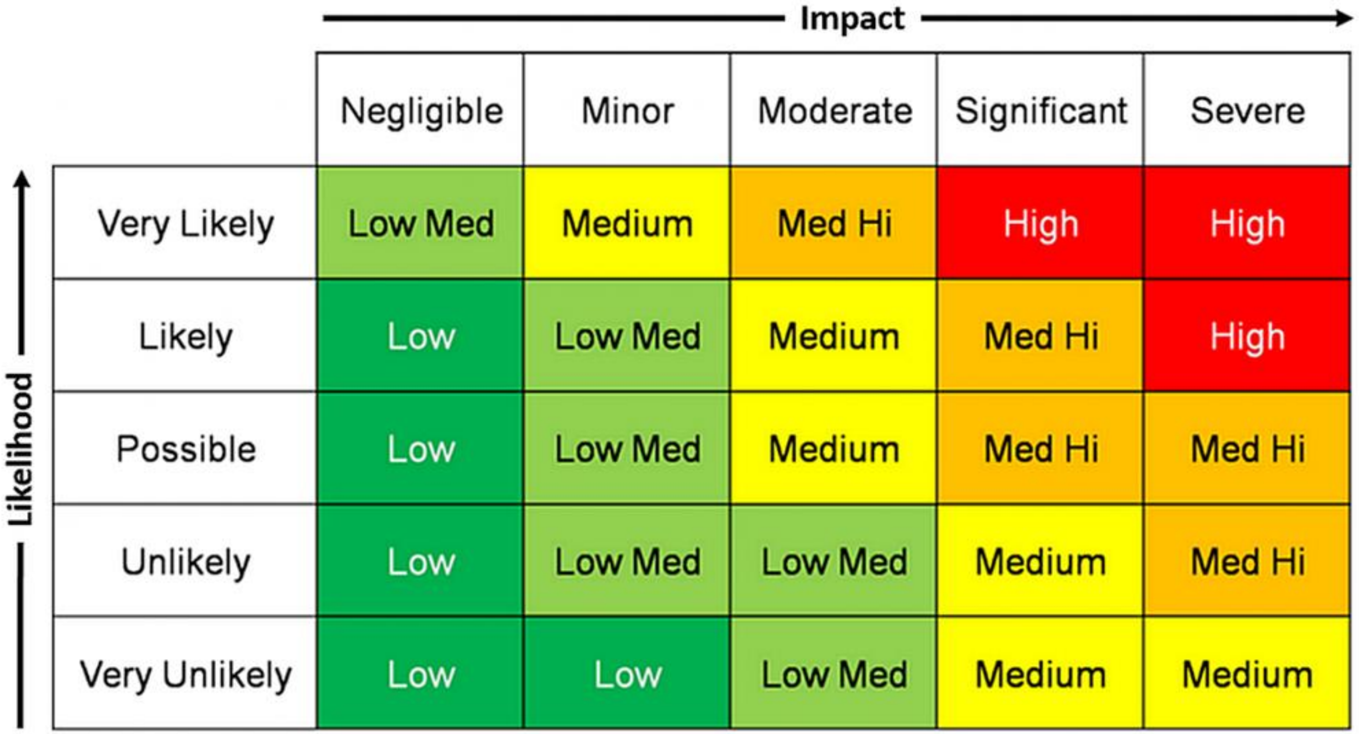
- A low-likelihood event with high impact may still deserve attention
- High-likelihood + high-impact = urgent risk

- If your **password manager** is weak,
  - Likelihood = Moderate (targeted phishing possible)
  - Impact = High (all secrets exposed)

  → **High Risk**

Likelihood vs Impact

- **Risk Matrix Grid:**
  - X-axis: Impact (Low to High)
  - Y-axis: Likelihood (Rare to Certain)
  - Each cell color-coded (Green = Low Risk, Yellow = Medium, Red = High)
- **Usage:**
  - Plot risks into matrix to determine response priority
  - Helps visualize what needs monitoring, mitigation, or immediate action



Impact

Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Low Likelihood, High Impact Events

Rare but Devastating

Can you think of any low likelihood but high Impact events?

Low Likelihood, High Impact Events

Rare but Devastating

- Tsunami / Earthquake / Volcano
- Bushfire / Dam Break / Tailings Failure
- Bridge or Building Collapse / Amusement Park Accident
- Election Hacked / Corrupt Judge / Fake Medical Degrees
- Pandemic / Nuclear Accident / Meteor Collision
- Insider Trading / Regulator Corruption / Politician Scandal
- Sports CTE / Rock Fishing / Dog Attacks
- Rise of Dictator / Revolution / School Shooting

Low Likelihood, High Impact Events

Rare but Devastating

Phase	**Key Questions**
In Advance	Were systems in place? Was the risk considered and mitigated?
Immediate	Were warning signs ignored? Was there a clear escalation or failure to act?
During	How was the event managed? Were there strengths in the response? Weaknesses?
Afterwards	Were lessons learned? Was there blame or meaningful change? Are the lessons lasting?

Why It Matters

- These risks test resilience, foresight, and preparedness
- A society that only reacts after **suffers avoidable consequences**

Passing / Accepting the Risk

- Risk Appetite
  - The amount and type of risk an organization is willing to pursue or accept to achieve its goals.
  - *“How much risk are we comfortable with?”*
- Risk Capacity
  - The maximum level of risk the organization can realistically bear without threatening its survival.
  - *“How much risk can we actually handle?”*
- Risk Tolerance
  - The acceptable variation in performance or outcomes within the appetite.
  - *“What deviation from the plan is still okay?”*

Risk Mitigation – Reducing the Threat

- Mitigation refers to actions taken to reduce the likelihood or impact of a risk.
  - It doesn’t eliminate the risk entirely
  - It makes the consequences less damaging or the event less likely

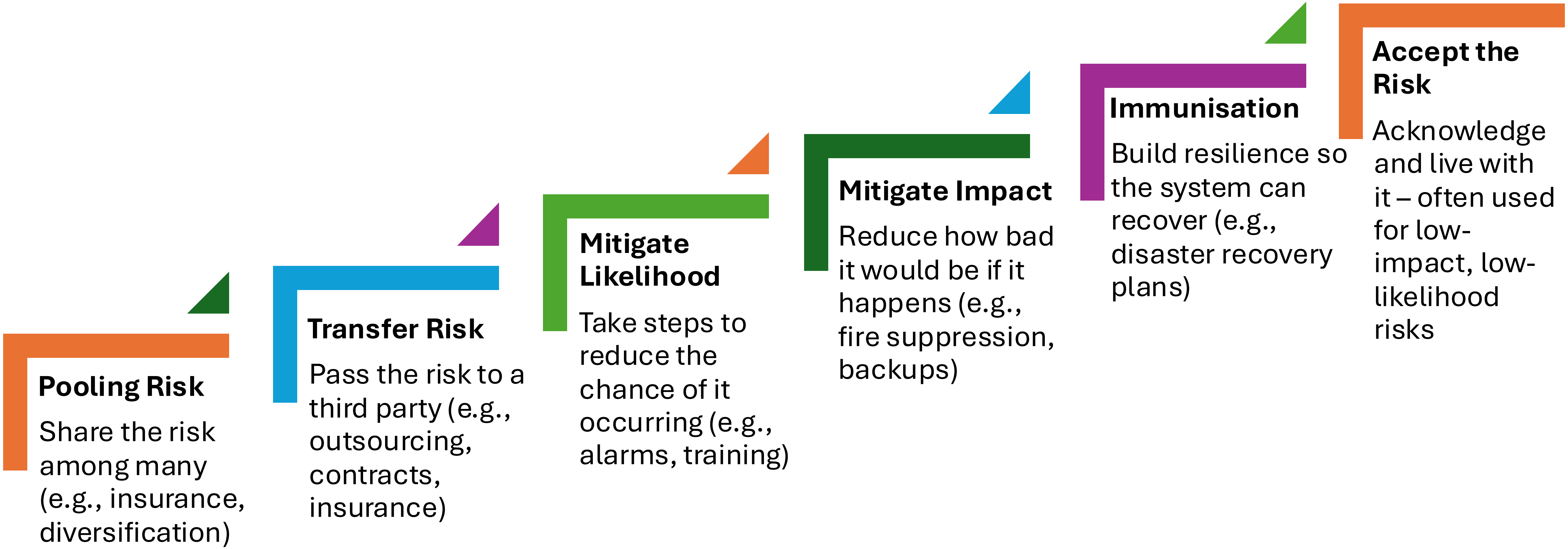
"Prepare, protect, and reduce harm."

Risk Mitigation – Reducing the Threat

Scenario	**Mitigation Measure**
Home security	Adding a gate or lock
Bank withdrawals	Installing ATM cameras
Public swimming pool	Posting lifeguards + warning signs
Crossing a street	Using traffic lights and zebra crossings
Pets in public	Leash laws to avoid dog attacks
Rock fishing	Warning signs, safety railings
Flood-prone areas	Levees, retention basins

"You can’t remove all risk, but you can prepare for it."

Stages of Resolving Risk



Pooling Risk

Share the risk among many (e.g., insurance, diversification)

Transfer Risk

Pass the risk to a third party (e.g., outsourcing, contracts, insurance)

Mitigate Likelihood

Take steps to reduce the chance of it occurring (e.g., alarms, training)

Mitigate Impact

Reduce how bad it would be if it happens (e.g., fire suppression, backups)

Immunisation

Build resilience so the system can recover (e.g., disaster recovery plans)

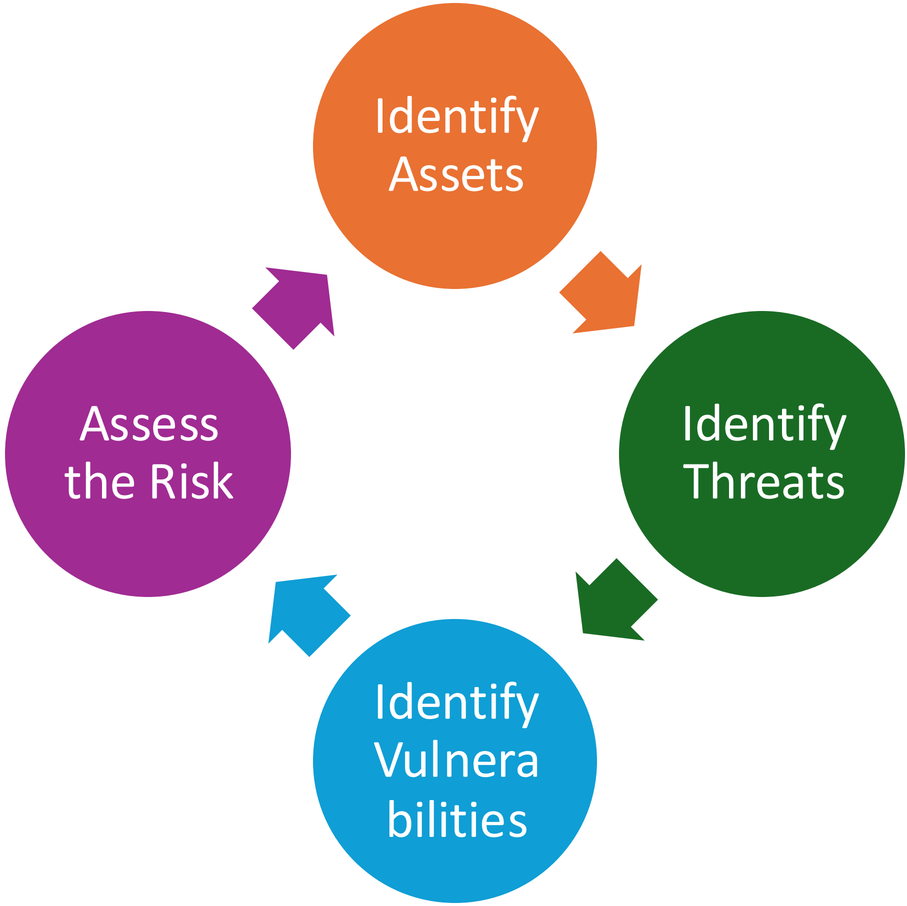
Accept the Risk

Acknowledge and live with it – often used for low-impact, low-likelihood risks

Resolving risk is not just about avoiding it, it's about choosing the right response.

Steps in Risk Analysis

- **Identify Assets** *(What are we protecting?)*
  - Data, systems, people, reputation, infrastructure
  - Ask: *What would hurt if we lost it?*
- **Identify Threats** *(What could go wrong?)*
  - Natural disasters, human error, cyberattacks, insider threats
  - Think in terms of who or what could cause harm
- **Identify Vulnerabilities** *(What are our weak spots?)*
  - Outdated systems, poor access controls, lack of training
  - Gaps that threats could exploit to harm assets
- **Assess the Risk** *(What's the likelihood + impact?)*
  - Combine threat + vulnerability to judge the real-world risk
  - Use qualitative or quantitative risk scoring



Type I and Type II Errors

	Truth: Innocent	**Truth: Guilty**
System Says YES (Action Taken)	❌ **Type I Error** (False Positive) – Wrongly flagged	✅ Correct Detection
System Says NO (No Action)	✅ Correct Rejection	❌ **Type II Error** (False Negative) – Missed the threat

- No system is perfect; decisions are based on incomplete or noisy information
- Probability thresholds, detection sensitivity, and imperfect models

Type I and Type II Errors

Context	**Type I Error (False Positive)**	**Type II Error (False Negative)**
Refugee Screening	Denying entry to an innocent person	Allowing a dangerous individual entry
Criminal Justice / Bail	Jailing the innocent	Releasing someone who reoffends
Drone Targeting System	Attacking a civilian	Failing to attack a confirmed threat
Medical Testing	Diagnosing illness when none exists	Missing a real illness

Over-engineering for one type of error can cause severe consequences from the other.

Thank you!
Questions?

Rahat Masood
rahat.masood@unsw.edu.au