Cipher Mode of Operations, Industrial Control System Security, RBAC, Malware-as-a-Service (Trend 2022-23)

ISC @ B Tech III CSE, SVNIT

Dhiren Patel

(April 2023)

Cipher Modes of Operations - What? Why?

- A mode of operation specifies how a block cipher can be used to encrypt a message that may be longer than one block.
- By design - Block cipher encrypts a fixed-size block of data at a time.
- These modes of operation provide different trade-offs between security, speed, and efficiency, and the choice of mode depends on the specific requirements of the application.

Block Cipher

- A block cipher (is a function which maps) n-bit plaintext blocks to n-bit ciphertext blocks; n is called the *block length*.
  - $E: \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$
- Various aspects of complexity
  - Data Complexity
  - Storage Complexity
  - Processing Complexity
- Cost of attack v/s value of information!!!

Modes of operations

block cipher encrypt fixed size blocks (e.g. DES – 64 bit, AES – 128 bit)

needs some way to encrypt/decrypt arbitrary large amounts of data in practise

NIST SP 800-38A defines 5 modes - **block** (and **stream)** modes to cover a wide variety of applications

can be used with any block cipher

(800-38D includes Galois/Counter Mode (GCM) <authenticated encryption> and GMAC <message authentication code>)

(800-38E - The XTS-AES Mode for Confidentiality on Storage Devices)

Various modes

- There are several modes of operation available for block ciphers, including:
- Electronic Codebook (ECB): The plaintext is divided into blocks and each block is encrypted separately. However, this mode is not secure because identical plaintext blocks will always be encrypted to the same ciphertext blocks.
- Cipher Block Chaining (CBC): In this mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. The first plaintext block is XORed with a random value called an initialization vector (IV). CBC is one of the most commonly used modes of operation.

Various modes

- Counter (CTR): This mode generates a unique key stream for each block of plaintext using a counter and a nonce. The nonce is a random value that is only used once, while the counter increments for each block. CTR is used in some disk encryption systems.
- Galois/Counter Mode (GCM): This mode combines the CTR mode with an authentication mechanism called Galois Message Authentication Code (GMAC). GCM is widely used in TLS encryption.

Various modes

- Output Feedback (OFB): In this mode, the block cipher is used to generate a key stream, which is then XORed with the plaintext to produce the ciphertext. OFB is similar to CTR mode, but it is less commonly used.
- Cipher Feedback (CFB): This mode is similar to OFB, but the feedback loop is different. The previous ciphertext block is encrypted and then XORed with the plaintext to produce the ciphertext. CFB is also less commonly used.

ECB

- ECB mode works by dividing the plaintext message into fixed-size blocks and encrypting each block separately with the same key. This means that identical plaintext blocks will always be encrypted to the same ciphertext blocks, which can lead to security vulnerabilities. ECB mode is not recommended for use in cryptography.

Electronic Codebook Book (ECB) mode of operation

message is broken into independent blocks

each block will be substituted <encrypted>, like a codebook, hence name ECB

each block is encoded independently of the other blocks

$C_i = E_K(P_i)$

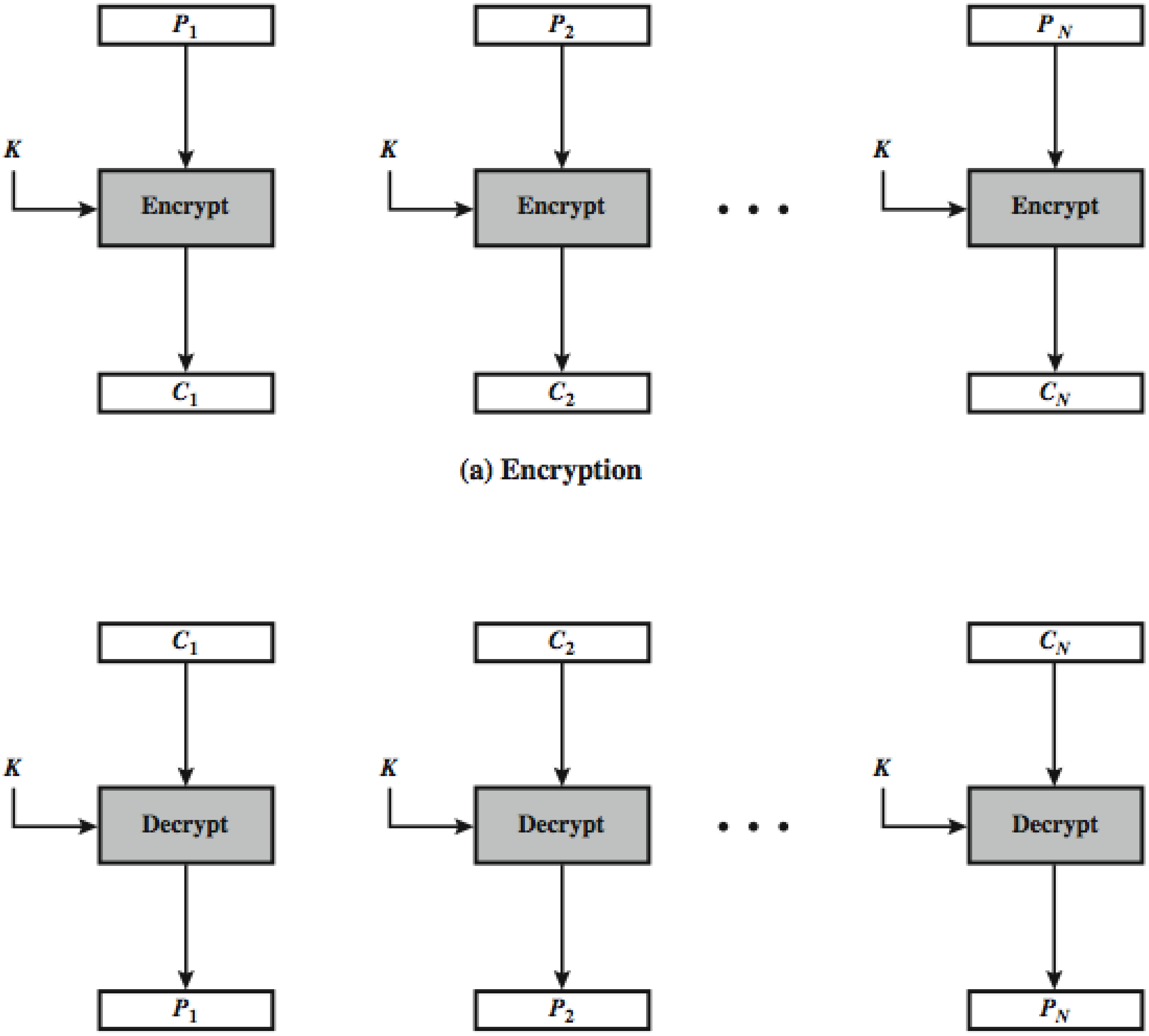
Message Padding

at the end, message must handle a possible last short block

which is not as large as blocksize of cipher

pad either with known non-data value (eg nulls, 1 followed by 0s)

Electronic Codebook Book (ECB

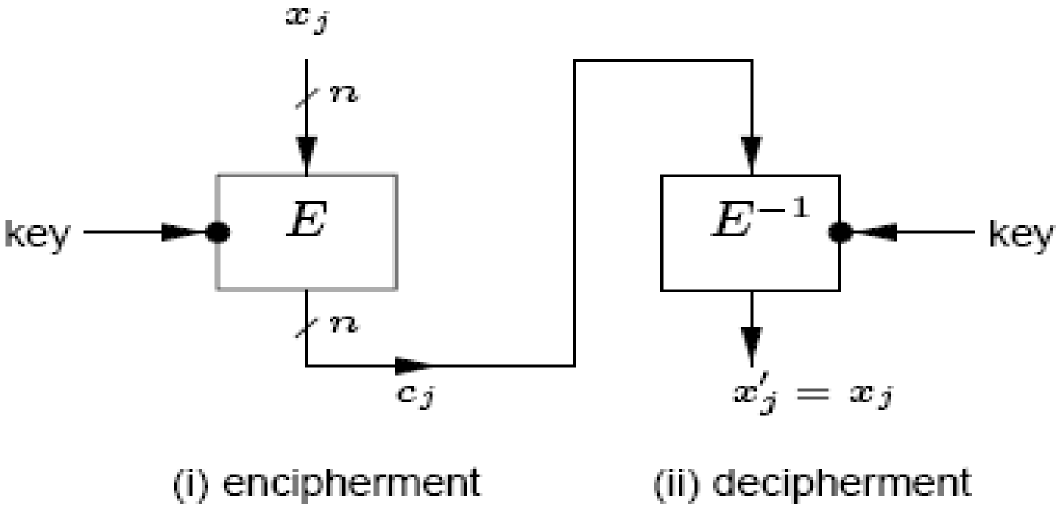


(a) Encryption

(b) Decryption

ECB (Electronics Codebook) Mode

- ❑ Encryption: for $1 \le j \le t$, $c_j \Leftarrow E_K(x_j)$.
- ❑ Decryption: for $1 \le j \le t$, $x_j \Leftarrow D_K(c_j)$.



properties

No Chaining dependencies:

- ❑Blocks are enciphered independently of other blocks. (Same key throughout entire msg)
- ❑Reordering ciphertext blocks results in correspondingly re-ordered plaintext blocks.

Error propagation:

- ❑One or more bit errors in a single ciphertext block affect decipherment of that block only.

Limitations of ECB

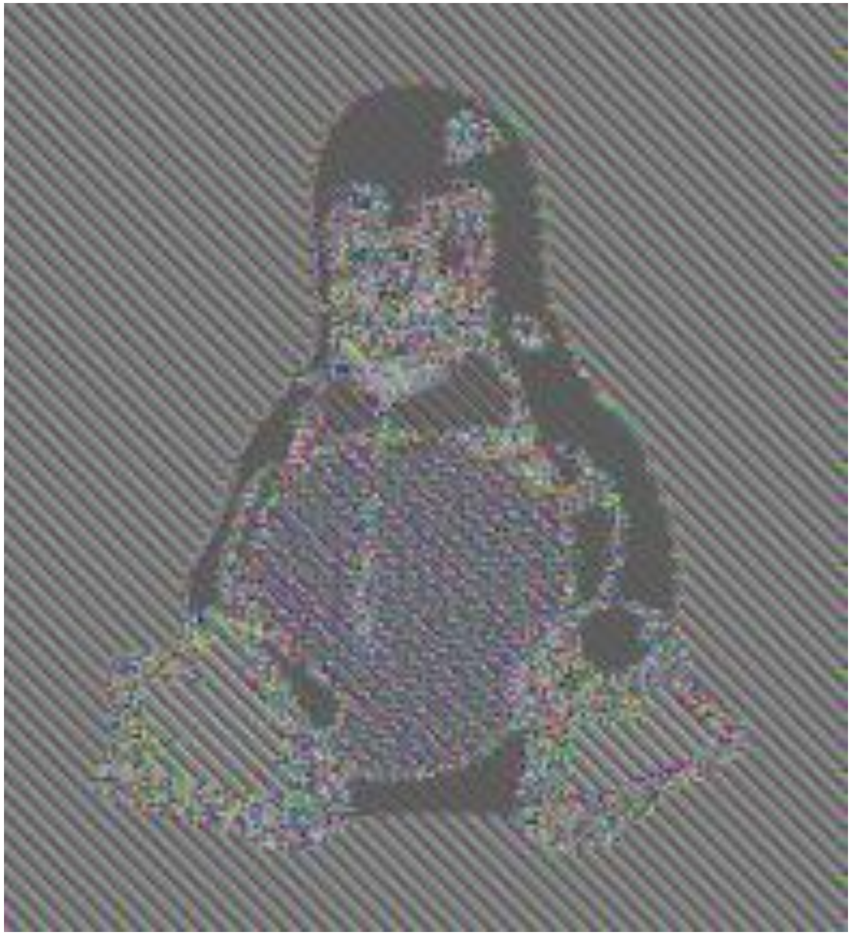
Identical blocks of plaintext will be encrypted as identical blocks of cipher text

- if aligned with plain text block
- particularly with data such as graphics
- or with messages that change very little, which become a code-book analysis problem

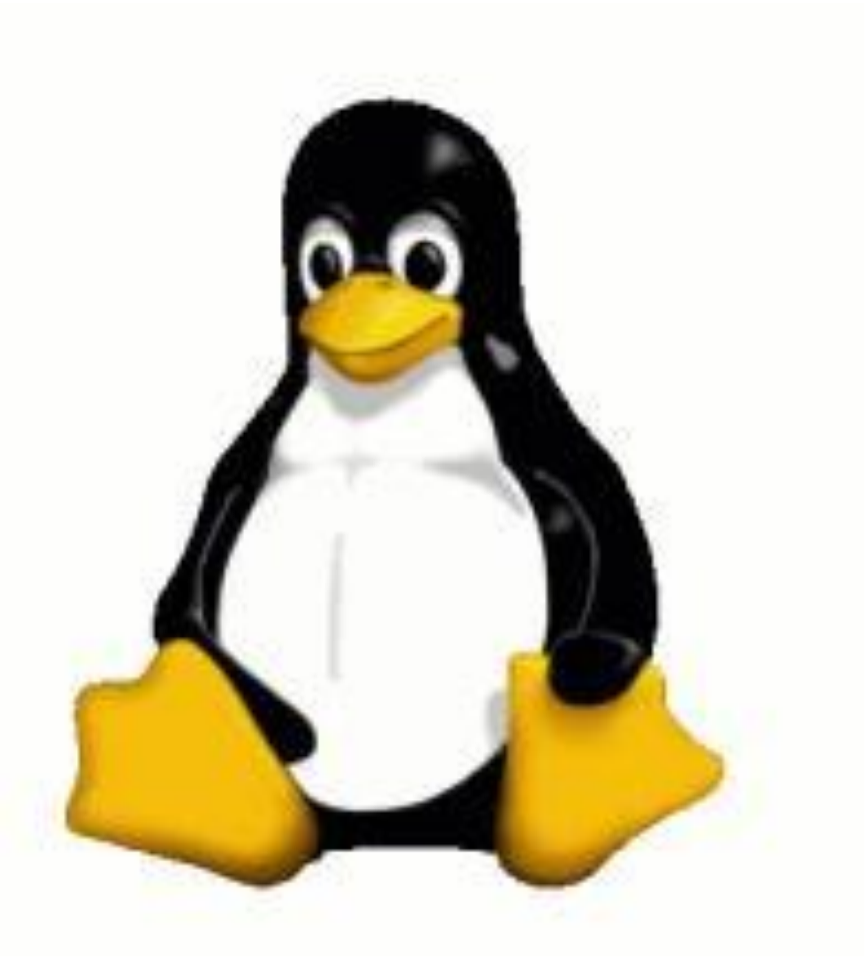
weakness is due to the encrypted message blocks being independent

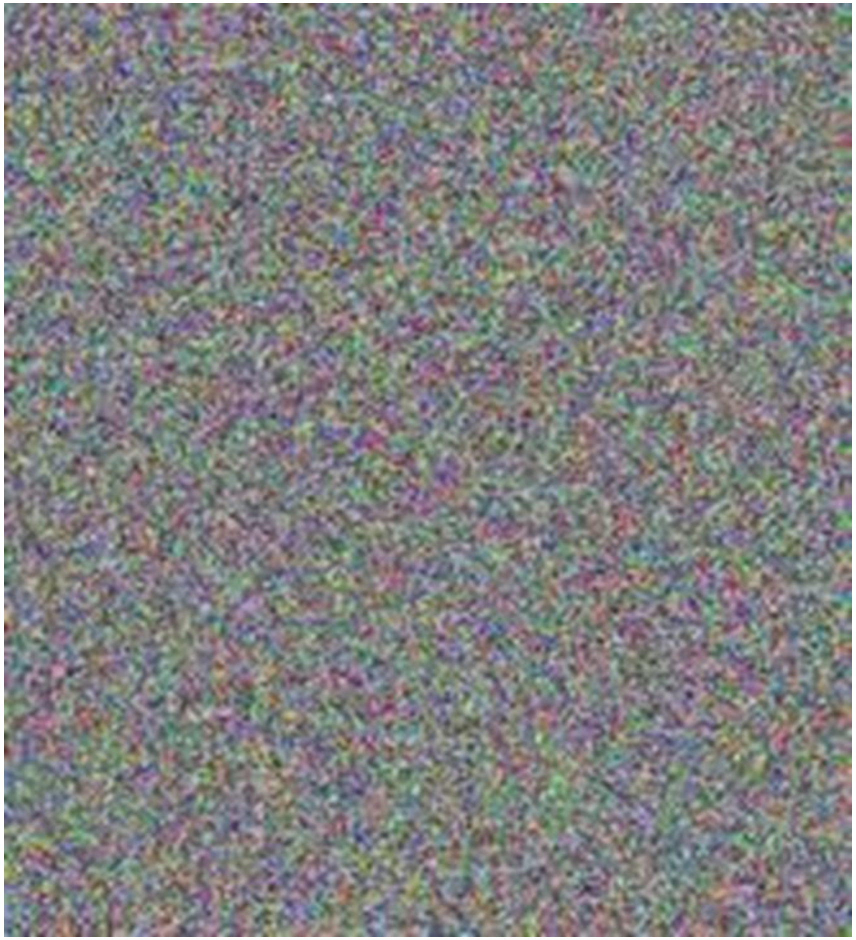
If attacker re-orders blocks it will not be detected by receiver!!

Encrypted with ECB

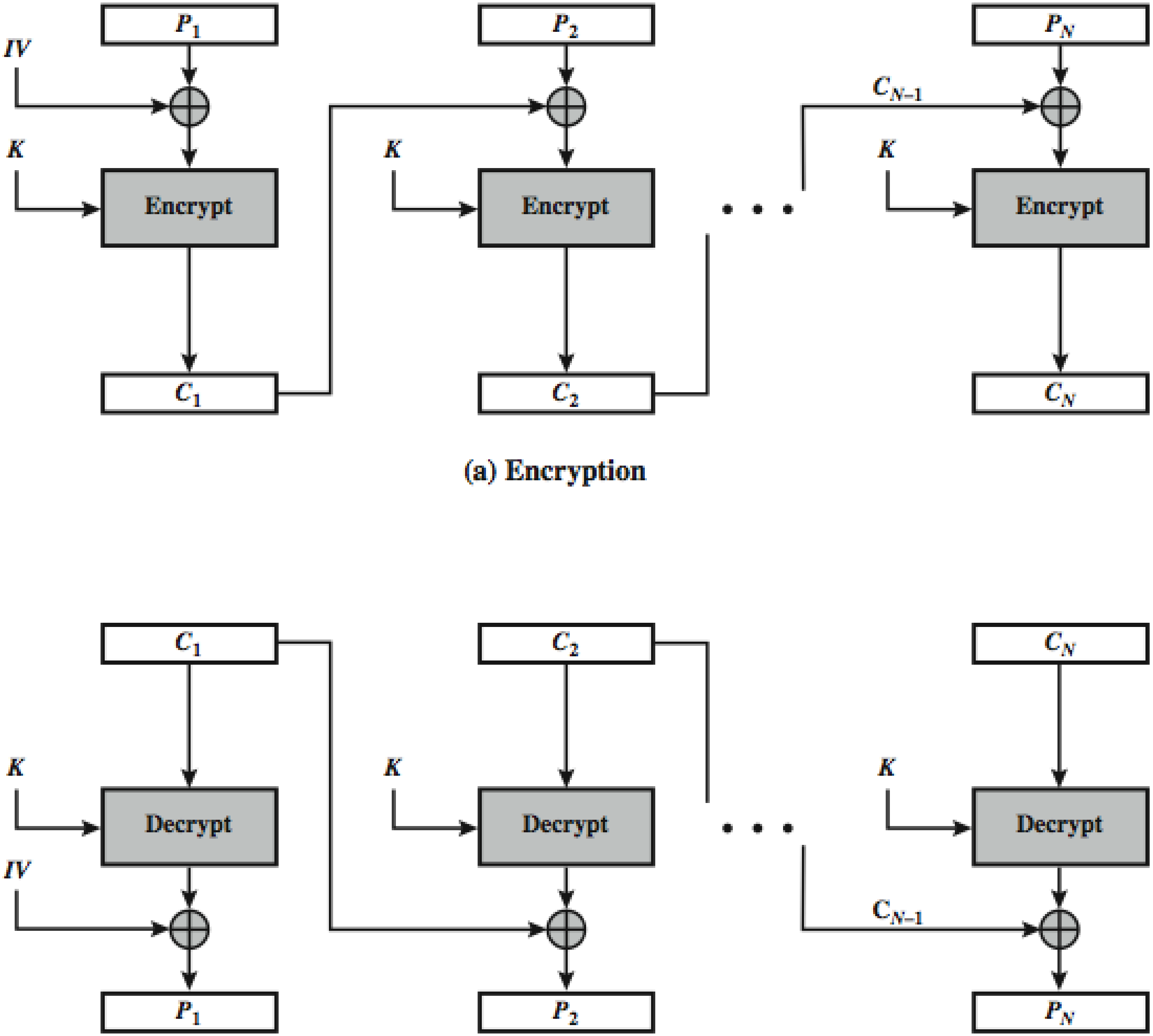


Original (left) and Encrypted with CBC





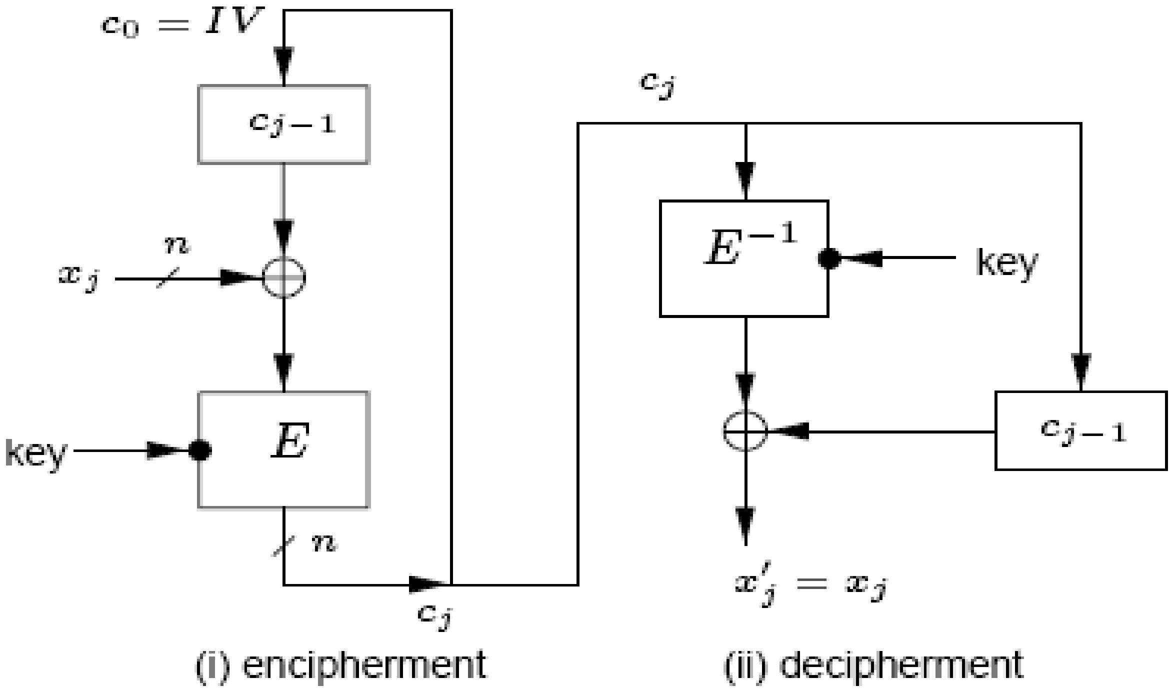
Cipher Block Chaining (CBC)



(a) Encryption

(b) Decryption

CBC (Cipher Block Chaining) Mode



CBC

- CBC stands for Cipher Block Chaining, which is a mode of operation used in symmetric key encryption. In CBC mode, each plaintext block is XORed with the previous ciphertext block before being encrypted, adding an extra level of randomness and preventing patterns from emerging in the ciphertext. This is done to provide confidentiality and integrity of data being transmitted or stored.
- Here's how CBC works:
- The first plaintext block is XORed with an Initialization Vector (IV) before being encrypted with the encryption algorithm, creating the first ciphertext block.
- For each subsequent plaintext block, it is XORed with the previous ciphertext block before being encrypted with the encryption algorithm to create the current ciphertext block.
- The process is repeated for all plaintext blocks, resulting in a series of ciphertext blocks.

CBC

- When decrypting the ciphertext, the reverse process is followed, with each ciphertext block being decrypted and then XORed with the previous ciphertext block to obtain the plaintext block.
- CBC mode is widely used in symmetric key encryption algorithms

Advantages and Limitations of CBC

as ciphertext block depends on **all** previous blocks;

any change to a block affects all the following (subsequent) ciphertext blocks

need of **Initialization Vector** (IV)

- which must be known to sender & receiver
- if sent in clear, attacker can change bits of first block, and change IV to compensate !!!!
- hence IV must be a fixed value
- or must be sent encrypted in ECB mode before rest of message

Any error in a particular ciphertext block will propagate and subsequent blocks may not be recovered

CBC

- Another advantage of CBC mode is that it supports parallel encryption and decryption of messages, as each block can be processed independently once the previous ciphertext block has been decrypted.
- However, CBC mode is vulnerable to certain attacks, such as padding oracle attacks or plaintext injection attacks, which can allow an attacker to modify the plaintext or extract information about it. These attacks can be mitigated by using appropriate padding techniques, authenticating the ciphertext with a message authentication code (MAC), or using a more secure mode of operation such as GCM (Galois/Counter Mode).

CBC

- One advantage of CBC mode is that it provides confidentiality and integrity protection for the encrypted message.
- The XOR operation between plaintext and ciphertext blocks makes it difficult for an attacker to modify the ciphertext without detection.
- Additionally, the IV ensures that even if the same plaintext message is encrypted multiple times with the same key, the resulting ciphertexts will be different.

OFB

- OFB mode, on the other hand, uses the block cipher to generate a keystream which is then XORed with the plaintext to produce the ciphertext. The keystream is generated by encrypting an initialization vector (IV) using the block cipher, and then feeding the resulting ciphertext back into the block cipher to generate the next keystream block. The IV and the key are not repeated for subsequent blocks, so OFB mode does not suffer from the same vulnerabilities as ECB mode.
- One advantage of OFB mode is that it allows for encryption and decryption of messages in parallel, since the keystream can be generated independently of the plaintext.

Advantages and Limitations of OFB

needs an IV which is unique for each use (??!!)

- if ever reuse attacker can recover outputs

bit errors do not propagate

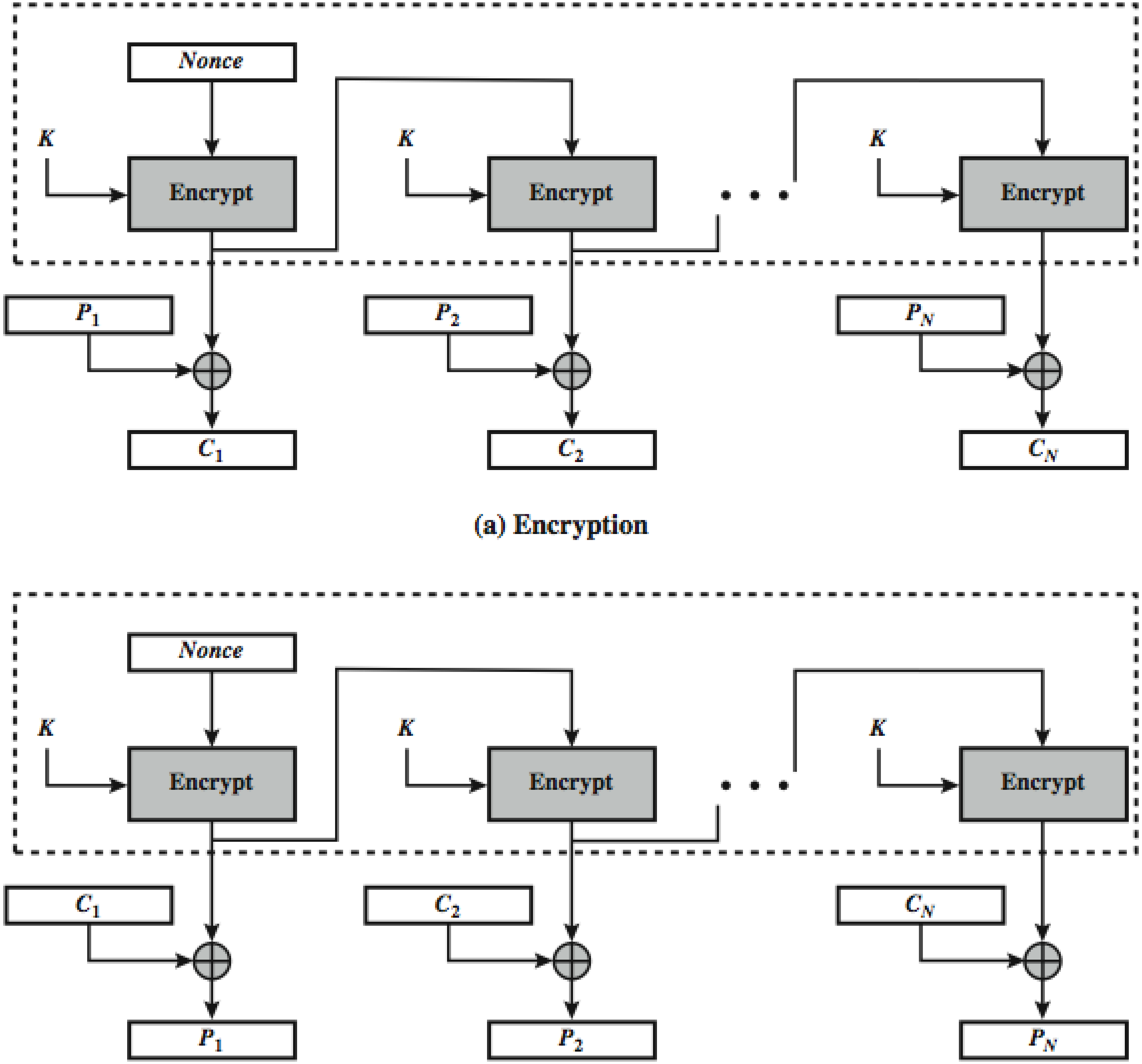
more vulnerable to message stream modification

sender & receiver must remain in sync

only use with full block feedback

- subsequent research has shown that only **full block feedback** (ie CFB-64 or CFB-128) should ever be used

Output FeedBack (OFB)



(a) Encryption

(b) Decryption

CTR

- The CTR mode of operation converts the block cipher into a stream cipher, generating a unique key stream for each block of plaintext using a counter and a nonce.
- The nonce is a random value that is only used once, while the counter increments for each block.

Counter (CTR)

a “new” mode, though proposed early on

similar to OFB but encrypts counter value rather than any feedback value

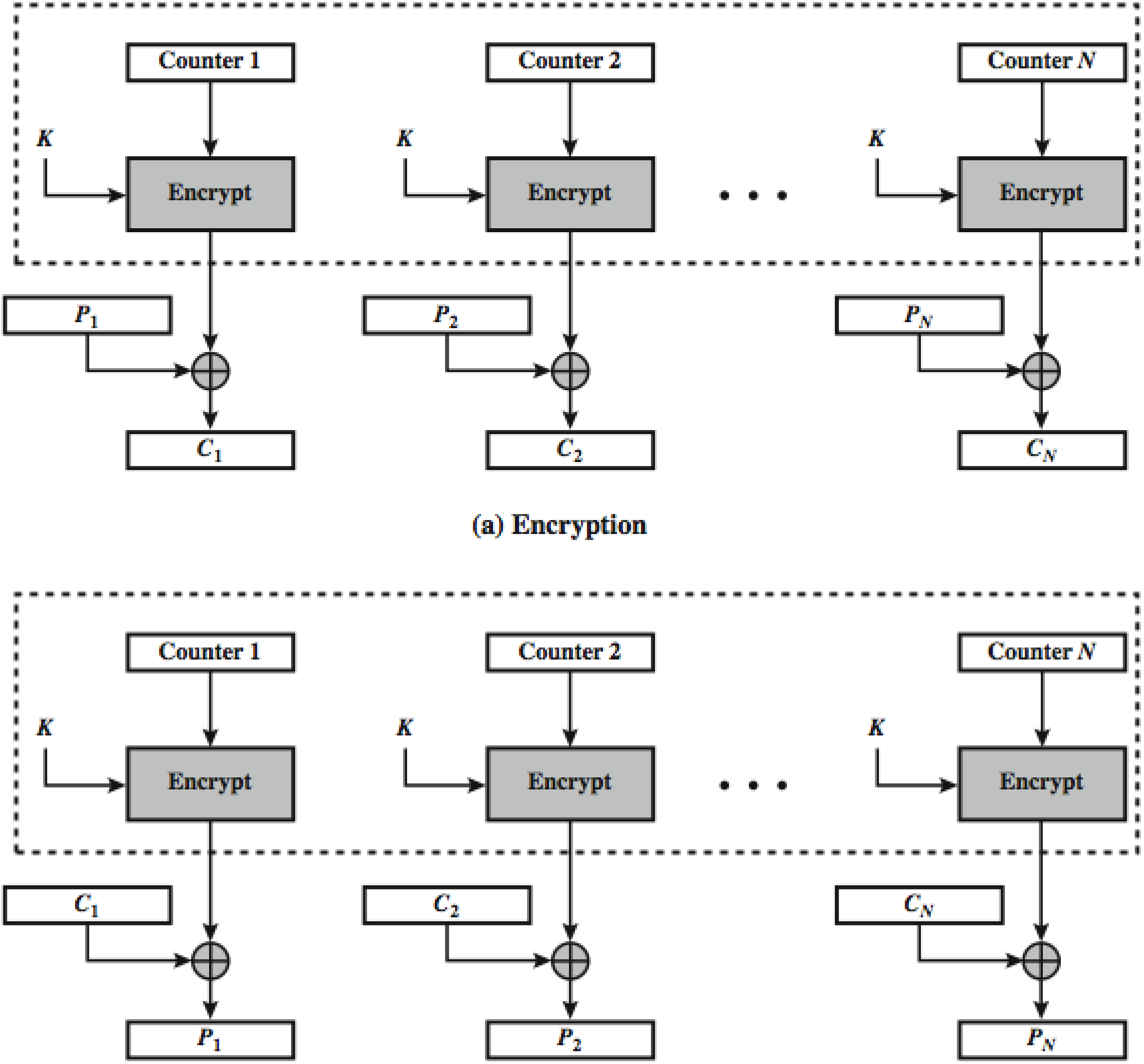
must have a different key & counter value for every plaintext block (never reused)

$O_i = E_K(i)$

$C_i = P_i \text{ XOR } O_i$

uses: high-speed network encryptions

Counter (CTR)



(a) Encryption

(b) Decryption

CTR

In CTR mode, a unique counter value is combined with a nonce and the encryption key to generate a key stream, which is then XORed with the plaintext message to produce the ciphertext. The counter is incremented for each block of plaintext, so each block has a unique key stream.

- One advantage of CTR mode is that it allows for random access to the encrypted message, since each block can be decrypted independently of the others once the key stream for that block has been generated. This makes it suitable for applications such as disk encryption or database encryption, where random access is required.

- Another advantage of CTR mode is that it supports parallel processing, allowing multiple blocks to be encrypted or decrypted at the same time.

CTR

- However, CTR mode does not provide message authentication or integrity protection, which means that an attacker can modify the ciphertext without detection.
- Therefore, it is important to use CTR mode in conjunction with a message authentication code (MAC) to ensure the integrity and authenticity of the encrypted message.
- Additionally, care must be taken to ensure that the counter value is not repeated,

GCM

- GCM (Galois/Counter Mode) is a mode of operation for block ciphers that provides both confidentiality and authenticity of encrypted messages. It is widely used in modern cryptographic applications, such as TLS encryption.
- GCM combines two cryptographic techniques: the Counter (CTR) mode of operation and the Galois Message Authentication Code (GMAC).

GMAC

- The GMAC mechanism provides authenticity of the encrypted message by generating a MAC (Message Authentication Code) for both the plaintext message and the associated data. The MAC is generated by hashing the key stream with a polynomial hash function called GHASH.
- The resulting ciphertext in GCM mode consists of the encrypted plaintext along with the authentication tag, which is the GMAC hash of the ciphertext and associated data. The authentication tag ensures that the ciphertext has not been tampered with or modified during transmission.

GCM

- One advantage of GCM mode is that it supports parallel processing, allowing multiple blocks to be encrypted or decrypted at the same time. Additionally, it provides both confidentiality and authenticity of the encrypted message, making it a secure and efficient mode of operation for block ciphers.
- However, it is important to note that GCM mode requires careful implementation to ensure its security properties are maintained. The nonce must be unique for each use, and the associated data must be authenticated to prevent attacks such as message replay or tag forgery.

Block Cipher Modes in Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of m plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed j bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding output.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Stream Cipher transmission

- A stream cipher eliminates the need to pad a message to be an integral number of blocks.
- It also can operate in real time.
- Thus, if a character stream is being transmitted, each character can be encrypted and transmitted immediately using a character-oriented stream cipher.
- cipher feedback (CFB) mode, output feed- back (OFB) mode, and counter (CTR) mode can be used for this.

CFB

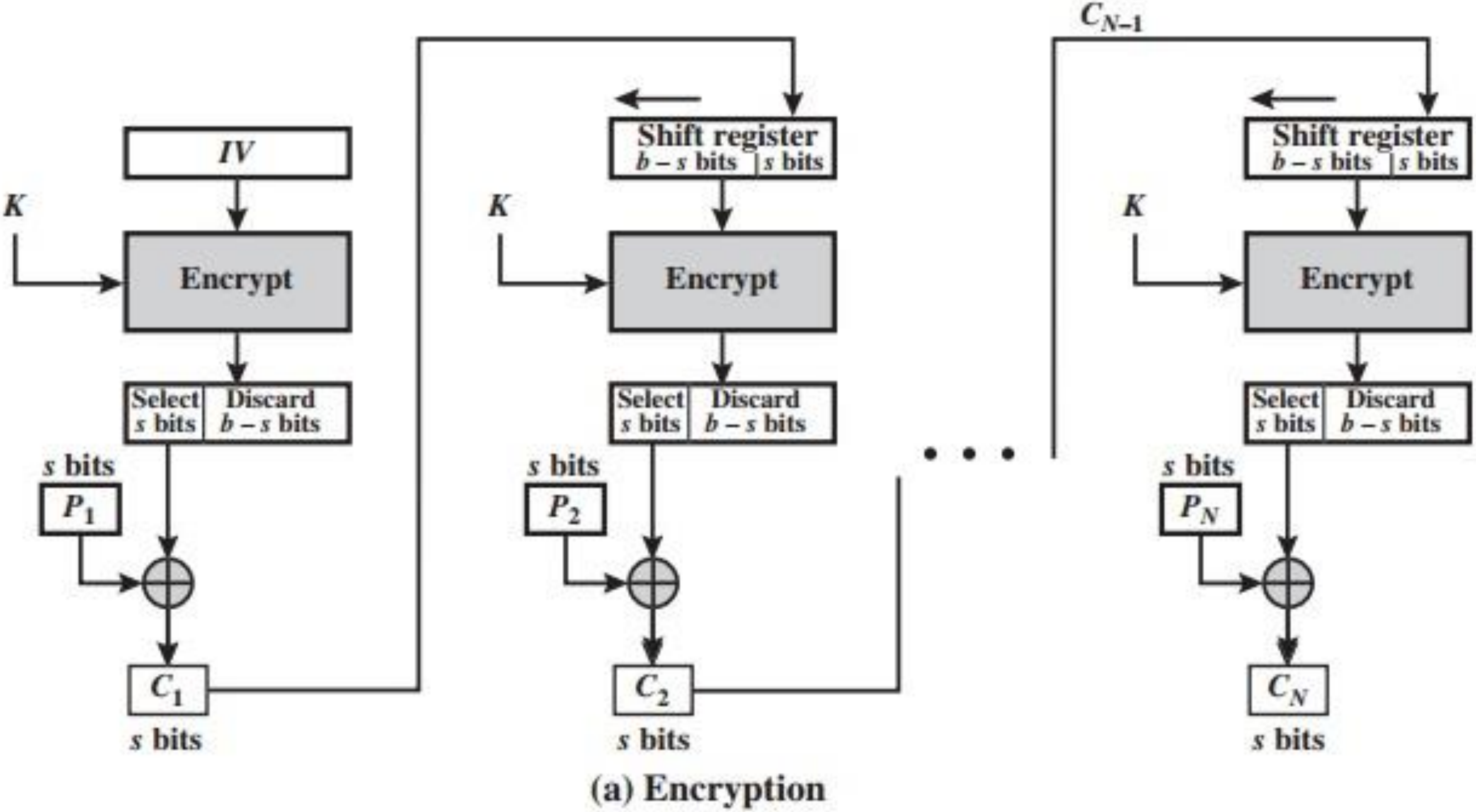
In the figure (next slide), the unit of transmission is *s* bits; a common value is *s* = 8.

As with CBC, the units of plaintext are chained together, so that the ciphertext of any plaintext unit is a function of all the preceding plaintext.

In this case, rather than blocks of *b* bits, the plaintext is divided into segments of *s* bits.

=

Cipher Feedback Mode (CFB)



(a) Encryption

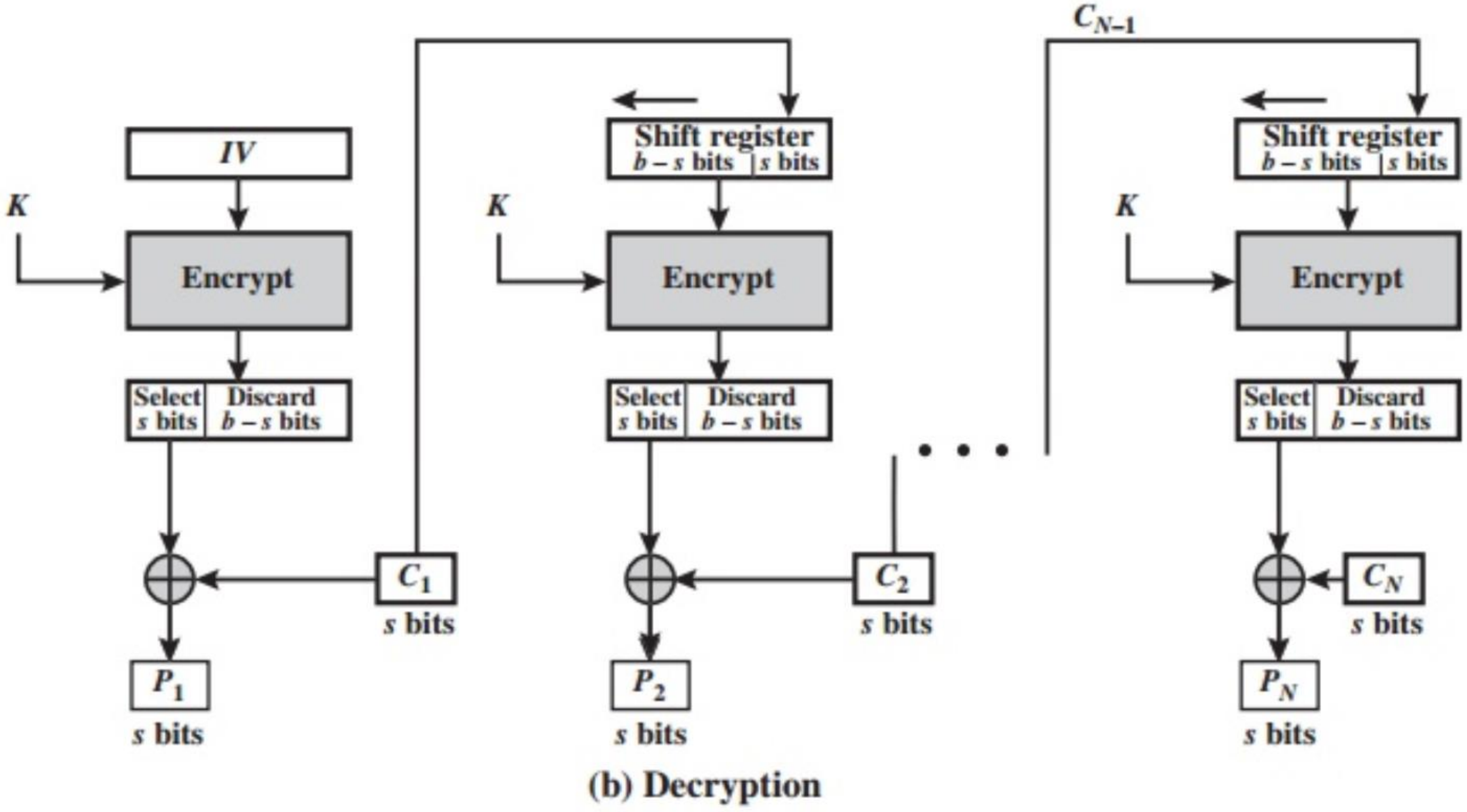
CFB

The input to the encryption function is a b-bit shift register that is initially set to some initialization vector (IV). The leftmost (most significant) s bits of the output of the encryption function are XORed with the first segment of plaintext P1 to produce the first unit of ciphertext C1, which is then transmitted.

In addition, the contents of the shift register are shifted left by s bits, and C1 is placed in the rightmost (least significant) s bits of the shift register. This process continues until all plaintext units have been encrypted.

For decryption, the same scheme is used, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext unit.

CFB - decryption



(b) Decryption

Industrial control system

- Industrial control system (ICS) is a collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes.
- Today the devices and protocols used in an ICS are used in nearly every industrial sector and critical infrastructure such as the manufacturing, transportation, energy, and water treatment industries.
- Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DCS) are most common ICSs.
- ICS Security focuses on ensuring the security and safe function of industrial control systems and its operators use

Supervisory Control and Data Acquisition (SCADA)

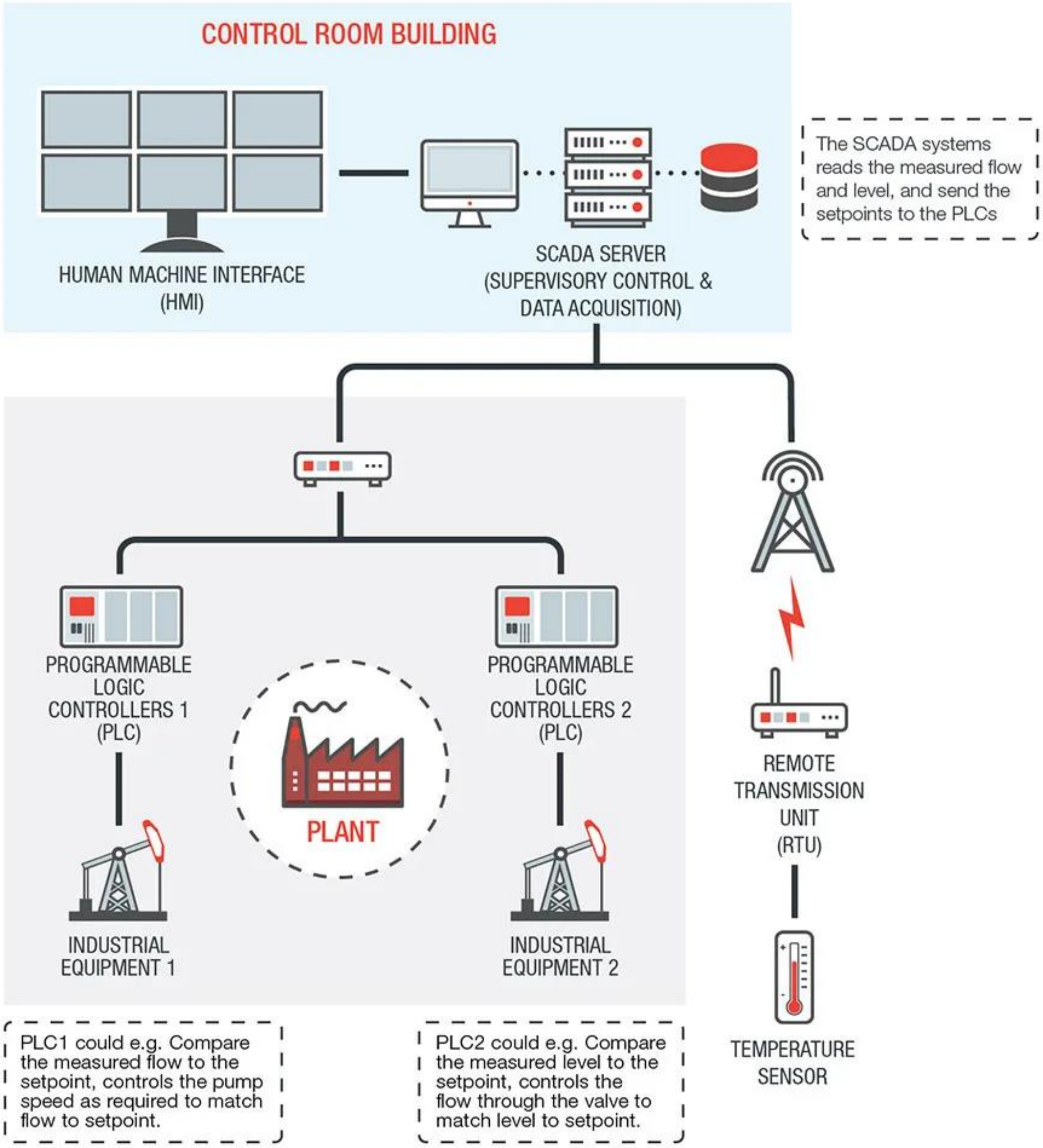
- The primary purpose of using SCADA is for long distance monitoring and control of field sites through a centralized control system

- SCADA systems are composed of devices (generally Programmable Logic Controllers (PLC) or other commercial hardware modules) that are distributed in various locations.

- SCADA systems can acquire and transmit data, and are integrated with a Human Machine Interface (HMI) that provides centralized monitoring and control for numerous process inputs and outputs.

- SCADA systems are commonly used in industries involving pipeline monitoring and control, water treatment centers and distribution, and electrical power transmission and distribution

SCADA


CONTROL ROOM BUILDING
HUMAN MACHINE INTERFACE (HMI)
SCADA SERVER (SUPERVISORY CONTROL & DATA ACQUISITION)
PROGRAMMABLE LOGIC CONTROLLERS 1 (PLC)
PLANT
PROGRAMMABLE LOGIC CONTROLLERS 2 (PLC)
REMOTE TRANSMISSION UNIT (RTU)
INDUSTRIAL EQUIPMENT 1
INDUSTRIAL EQUIPMENT 2
TEMPERATURE SENSOR

The SCADA systems reads the measured flow and level, and send the setpoints to the PLCs

PLC1 could e.g. Compare the measured flow to the setpoint, controls the pump speed as required to match flow to setpoint.

PLC2 could e.g. Compare the measured level to the setpoint, controls the flow through the valve to match level to setpoint.

Distributed Control System (DCS)

- This is a system that is used to control production systems that are found in one location
- Each DCS uses a centralized supervisory control loop to manage multiple local controllers or devices that are part of the overall production process. This gives industries the ability to quickly access production and operation data. And by using multiple devices within the production process, a DCS is able to reduce the impact of a single fault on the overall system.
- A DCS is commonly used in industries such as manufacturing, electric power generation, chemical manufacturing, oil refineries, and water and wastewater treatment.

ICS and IIoT

- Because ICS often support critical infrastructure, they cannot easily be taken down for security updates and so often remain unpatched and vulnerable
- Industrial systems, including critical infrastructure, are increasingly being networked and outfitted with computing and communications technologies.
- IIoT is about networking non-computing devices and making it possible for them to exchange data over the Internet
- The trend to IT/OT convergence means that systems used for data-centric computing

Security of DCS, SCADA

- ICS security focuses on ensuring the security and safe function of industrial control systems
- Operational Technology (OT) variables include the hardware and software systems that monitors and controls physical devices in the field.
- The convergence of IT and OT provides enterprises greater integration and visibility of the supply chain– which include their critical assets, logistics, plans, and operation processes.
- On the flip side, however, the convergence of OT and IT allows easier access to these two components that are targets of cybercriminals.

ICS Security

- ICS security includes a wide range of practices including:

1. Asset inventory and detection
2. Vulnerability management
3. Network intrusion protection and detection
4. Endpoint detection and response
5. Patch management
6. User and access management

ICS Security

ICS security differs from traditional IT security in several ways:

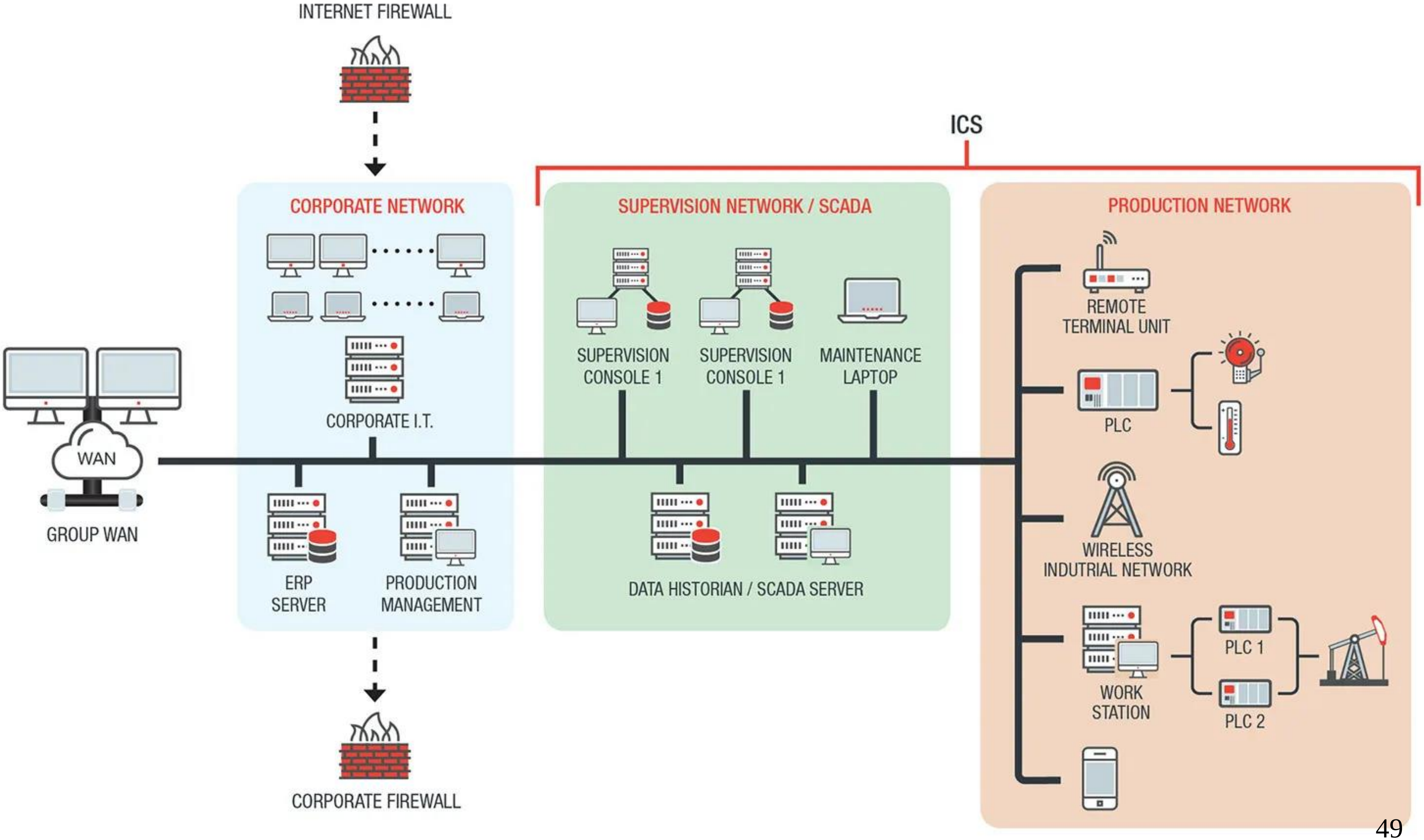
The type of devices protected are often sensitive to unintended changes or interaction, including a whole new class of OT assets known as embedded equipment, and are typically much older than IT systems.

Risks are not only to information confidentiality but especially to the availability and integrity of the process or safety to personnel and property.

ICS vulnerabilities (detect)

- **Policy and procedure**–incomplete, inappropriate, or non-existent security policy, including its documentation, implementation guides (e.g., procedures), and enforcement
- **Architecture and design**–design flaws, development flaws, poor administration, and connections with other systems and networks
- **Configuration and maintenance**–misconfiguration and poor maintenance
- **Physical**– lack of or improper physical access control, malfunctioning equipment
- **Software development**–improper data validation, security capabilities not enabled, inadequate authentication privileges
- **Communication and network**–non-existent authentication, insecure protocols, improper firewall configuration

Securing ICS



AI in Cyber Security

- cyberattacks grow in volume and complexity
- Threat Intelligence - threat landscape demands visibility, automation and contextual insights with a robust, open approach
- AI is changing the game for cybersecurity, analyzing massive quantities of risk data to speed response times and augment under-resourced security operations.
- technologies like machine learning and natural language processing provide rapid insights to cut through the noise of daily alerts, drastically reducing response times
- Power of cognitive AI is used to investigate indicators of compromise and gaining critical insights.

Access Management

- Access Management technologies can be used to enforce authorization polices and decisions, especially when existing field devices do not provided sufficient capabilities to support user identification and authentication.
- These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials.

Anti-Virus

- Anti-Virus, Anti-Malware:
- Use signatures or heuristics to detect malicious software.
- Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations.
- To minimize the impact to system availability, all products should first be validated within a representative test environment before deployment to production systems.
- Boot Integrity: secure methods to boot a system and verify the integrity of the operating system and loading mechanisms

Audits

- Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.
- Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations.
- Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.

Authorization and RBAC

- Role-based access control (RBAC) is a method of restricting network access based on the roles of individual users within an enterprise
- The device or system should restrict read, manipulate, or execute privileges to only authenticated users who require access based on approved security policies.
- Role-based Access Control (RBAC) schemes can help reduce the overhead of assigning permissions to the large number of devices within an ICS.
- For example, IEC 62351 provides examples of roles used to support common system operations within the electric power sector , while IEEE 1686 defines standard permissions for users of IEDs.
- Account Use Policies: Configure features related to account use like login attempt lockouts, specific login times, etc.

Data back up and protection

- Take and store data backups from end user systems and critical servers.
- Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.
- Protect sensitive data-at-rest with strong encryption.
- Maintain and exercise incident response plans, including the management of 'gold-copy' back-up images and configurations for key systems to enable quick recovery and response from adversarial activities that impact control, view, or availability.
- Data Loss Prevention (DLP) technologies can be used to help identify adversarial attempts to exfiltrate operational information, such as engineering plans, trade secrets, recipes, intellectual property, or process telemetry.

Filter Network Traffic

- Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.
- Perform inline allow/denylisting of network messages based on the application layer (OSI Layer 7) protocol, especially for automation protocols.
- Application allowlists are beneficial when there are well-defined communication sequences, types, rates, or patterns needed during expected system operations.
- Application denylists may be needed if all acceptable communication sequences cannot be defined, but instead a set of known malicious uses can be denied (e.g., excessive communication attempts, shutdown messages, invalid commands).

Human User Authentication

- Require user authentication before allowing access to data or accepting commands to a device.
- While strong multi-factor authentication is preferable, it is not always feasible within ICS environments. Performing strong user authentication also requires additional security controls and processes which are often the target of related adversarial techniques (e.g., Valid Accounts, Default Credentials).
- Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.

Multi factor authentication

- Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.
- Within industrial control environments assets such as low-level controllers, workstations, and HMIs have real-time operational control and safety requirements which may restrict the use of multi-factor.
- Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

Safety Instrumented Systems

- Utilize Safety Instrumented Systems (SIS) to provide an additional layer of protection to hazard scenarios that may cause property damage.

- A SIS will typically include sensors, logic solvers, and a final control element that can be used to automatically respond to an hazardous condition . Ensure that all SISs are segmented from operational networks to prevent them from being targeted by additional adversarial behavior.

SCM

- Implement a supply chain management program, including policies and procedures to ensure all devices and components originate from a trusted supplier and are tested to verify their integrity.
- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.
- Utilize watchdog timers to ensure devices can quickly detect whether a system is unresponsive.

Security as a Service
Attack as a Service
Malware as a Service
XaaS

Defending against the new malware "as-a-service" global economy

- While Russia-based threat actor groups spread misinformation and launched multiple cyberattacks against Ukraine, China-based (and likely sponsored) threat actor groups attacked hardware security products made by nearly every company in the cybersecurity and infrastructure industries.
- During this time, the cybercriminal economy has increasingly transformed into an industry. Information technology companies have shifted to "as-a-service" offerings, and the cybercrime ecosystem has done the same.
- Access brokers, ransomware, information-stealing malware, malware delivery, and other elements of cybercrime operations have lowered barriers to entry for would-be cybercriminals.
- Chat-GPT has further made the entry easier for bad actors.

Malware as a Service

- Criminal marketplaces such as Genesis enable entry-level cybercriminals to purchase malware and malware deployment services and sell stolen credentials and other data in bulk. Access brokers are increasingly selling vulnerable software exploits and credentials to other criminal organizations.
- This industrialization of ransomware has allowed ransomware “affiliates” to evolve into professional operations specializing in exploitation. These professional groups specialize in gaining (or purchasing) access for any motivated actor willing to pay—or, in some cases, multiple actors with multiple motives.

XaaS

- Access-as-a-service
- Gaining access to compromised accounts and systems in bulk through RDP and VPN credentials, web shells, and exploitable vulnerabilities
- Malware-as-a-service
- Facilitating the distribution of malware within specific regions or sectors with watering-hole attacks, crossover with access-as-a-service listings, and other vulnerabilities
- OPSEC-as-a-service
- Bundled services provided by threat actors designed to hide Cobalt Strike infections to minimize the risk of detection

XaaS

- Phishing-as-a-service
- How threat actors are offering end-to-end services for cloned sites, hosting, emails to bypass spam filters, and other phishing campaigns
- Crypting-as-a-service
- Common on many forums, crypting as a service involves the use of encrypted malware to bypass detection for a one-time purchase or subscription
- Scamming-as-a-service
- Designed as classified ads, scamming kits and services help threat actors pose as support specialists for cryptocurrency scams

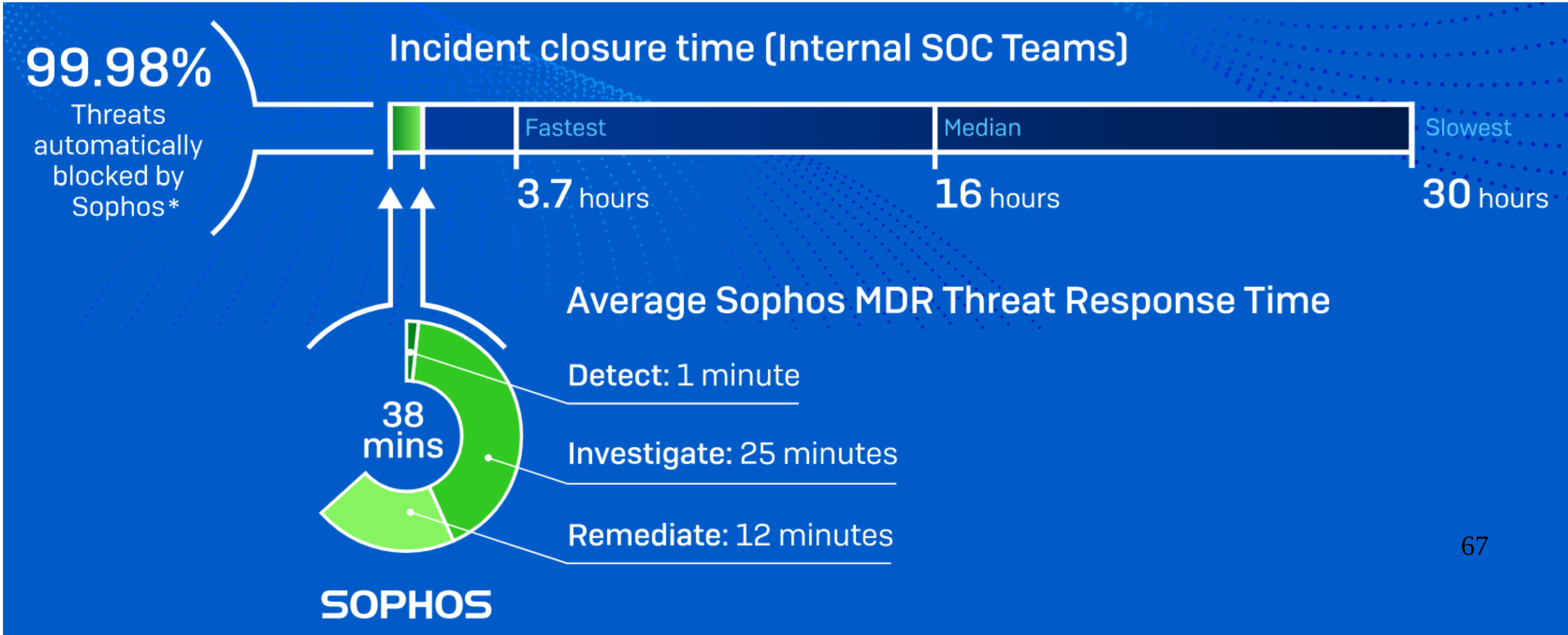
XaaS

- Vishing-as-a-service
- How threat actors offer to rent voice systems to receive calls where victims opt out and speak to a bot, rather than a human
- Spamming-as-a-service
- Infrastructure designed to build or manage bulk spamming services through a variety of mechanisms, including SMS and email
- Scanning-as-a-service
- Offering access at discount prices for legitimate commercial tools such as Metasploit and Burp Suite to find and exploit vulnerabilities

Managed Detection and Response (MDR)

(Sophos Group plc is a British-based security software and hardware company)

- a fully managed service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more (SOC – Security Operations Centre)



MDR Offerings

- single dashboard for real-time alerts, reporting, and management
- compatible with a growing list of security telemetry providers such as Amazon Web Services (AWS), Check Point, CrowdStrike, Darktrace, Fortinet, Google, Microsoft, Okta, Palo Alto Networks, Rapid7, and many others
- NDR (Network Detection and Response) identifies potential attacker activity inside your network (works as an add-on to Sophos MDR)
- Analysts with critical visibility and context for seeing the entire attack path, enabling a faster, more comprehensive response to security threats

Network Detection and Response

- Monitors network traffic to identify suspicious network flows - with the ability to detect potentially malicious behaviors, Sophos NDR identifies:
- Unprotected Devices – It (NDR) identifies legitimate devices that haven’t been protected and could be used as entry points for cyberattacks.
- Rogue Assets – In addition to monitoring traffic to unprotected devices, it identifies unauthorized devices that communicate across the network.

NDR

- IoT and OT Sensors – Internet of Things (IoT) and operational technology (OT) devices represent challenges to threat monitoring because many of these devices cannot support an endpoint protection agent. It (NDR) monitors data from IoT and OT devices to detect attacker activity.
- Zero-Day Attacks – It has a process for detecting zero-day C2 servers used by attackers based on patterns found in session packet size, direction, and interarrival times. (Encrypted Payload Analytics (EPA))
- Insider Threats – It provides visibility into network traffic flows and data exfiltration that may initially appear “normal” from those on the inside.

Okta

- Okta, Inc. is an American identity and access management company based in San Francisco.
- It provides cloud software that helps companies manage and secure user authentication into applications, and for developers to build identity controls into applications, website web services and devices.
- Okta is a customizable, secure, and drop-in solution to add authentication and authorization services to your applications

Characterization v/s Fingerprinting

- Characterizing is the act of collecting, analyzing, and/or storing information intended to be used in describing behavior and/or characteristics pertaining to a device.
- Fingerprinting is the act of collecting information intended to help uniquely identify a device type.

IIoT (Industrial Internet of Things)

- The sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications
- Sensor - A device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument.
- A sensor is a device, which responds to an input quantity by generating a functionally related output usually in the form of an electrical or optical signal

IIoT Security

- communications and data integrity to ensure that information is not modified in transit
- authentication and access control to ensure that only known, authorized systems can exchange information
- command register that maintains an independent, immutable record of information exchanges between sources (producers and consumers) and operators
- malware detection to monitor information exchanges and processing to identify potential malware infections
- behavioral monitoring to detect deviations from operational norms
- analysis and visualization processes to monitor data, identify anomalies, and alert operators

(Additional) - Secret Sharing

- Secret sharing schemes are cryptographic protocols that allow a group of participants to share a secret in such a way that only authorized subsets of the participants can reconstruct the secret.
- The idea is to split the secret into several pieces, called shares, and distribute them among the participants in such a way that only a subset of them, called the qualified set, can recover the secret.

Secret Sharing example

- In general, a secret may be split into n shares (for n shareholders), out of which, a minimum of t, (t < n) shares are required for successful reconstruction.
- E.g. Line
- For instance, to reconstruct a curve of degree 1 (a straight line), we require at least 2 points that lie on the line.
- Distribute 4 points of a line each to 4 participants. To reconstruct line, any two points are required!!

Some References

- Sophos (https://www.sophos.com/)
- Fortinet (https://www.fortinet.com/)
- Verve (https://verveindustrial.com/)
- NIST (SP) 800-82 (Standard)