Introduction to Computer Security

What is Computer Security? (1 of 3)

Oregon State University
College of Engineering

It is the “Art & Science” of protecting or securing computer systems

What is Computer Security? (2 of 3)

Oregon State University
College of Engineering

It is the "Art & Science" of protecting/securing computer systems

- What does protecting or securing mean?
  - Examples:
    - protecting your computer against viruses or other malware
    - protecting your information (e.g., tax returns) from being taken or accessed by others (*unauthorized)*

What is Computer Security? (3 of 3)

Oregon State University
College of Engineering

It is the "Art & Science" of protecting/securing computer systems?

- Why is it considered both "Art and Science"
  - while many things in computer security are science or engineering, some aspects remain an 'Art'
  - Examples: security mindset, designing ciphers, etc

Why do we need computer security? (1 of 2)

Oregon State University
College of Engineering

Because we need to protect or secure computers against …. adversaries

Why do we need computer security? (2 of 2)

Oregon State University
College of Engineering

Because we need to protect or secure computers against …. adversaries

- Who are these *adversaries?*
  - Prying family/friends (?) ☺
  - Mischief makers (script kiddies)
  - Hackers (fame/money/…)
  - Hacktivists (hackers but motivated by a cause)
  - Organized crime
  - Nation states
  - …

Why is computer security challenging?

Oregon State University
College of Engineering

- Both systems to be protected and security mechanisms can be quite complex and subtle
- Security mechanisms themselves might become targets or introduce unintended weaknesses
- A single weakness can bring down the system – defenders have to work harder
- Systems, environments, and adversaries are constantly evolving/changing
- Security often tends to be an afterthought rather than designed in
- Users play a crucial role and usable security is hard
- ….

Summary

Oregon State University
College of Engineering

- Computer security is the art and science of protecting computer systems against potential adversaries

- Computer security is challenging because of ever changing systems, environments and adversaries, and complexity of systems among other things.

Key Security Notions/Attributes

Confidentiality

Oregon State University
College of Engineering

- Preventing unauthorized access or disclosure of data/information
  - Keeping data (and metadata) confidential to authorized parties

- Example:
  - if corporate spies or outsiders gain access to coca-cola's formula that would be a serious loss of confidentiality

Privacy

Oregon State University
College of Engineering

- Preventing unauthorized access or disclosure of information/data **about people**

- An individual's right to decide who gets access to information/data about them

- Examples:
  - if attackers breach Target to steal credit card numbers from Target or breach IRS to steal SSN that would be a violation of privacy
  - if a hospital shares your medical information with others without your permission that would be a breach of privacy

Integrity

- Preventing against unauthorized modifications
  - Data Integrity (integrity)
  - Origin Integrity (authentication)
  - System Integrity

- Examples:
  - overwriting your bank balance file/database
  - forged from address in e-mail, junk call, IP packet
  - malware on computer (unauthorized change to system)

Availability

- Ensuring timely availability of (data, system service etc.)

- Example:
  - Denial-of-service attack taking down a network/server

Authenticity

Oregon State University
College of Engineering

- Property of being genuine; can be verified and trusted
  - How is this related to integrity?
- Example:
  - A pirated copy of software

Accountability

Oregon State University
College of Engineering

- Requirement for entity actions to be traced uniquely to that entity
- Non-repudiation
  - one cannot repudiate one's actions
- Example:
  - paying with a credit card and later claiming never having done the transaction

Summary

Oregon State University
College of Engineering

- Key Security Attributes:
  - Confidentiality
  - Integrity
  - Availability
  - Privacy
  - Authenticity
  - Accountability
- Confidentiality, Integrity and Availability are remembered as ‘CIA’
- These notions are not all independent
  - Confidentiality or Secrecy <-> Privacy
  - Integrity <-> Authenticity

Some Computer Security Terminology

Asset

Oregon State University
College of Engineering

- Something of value

- Examples:
  - data, system, service, networks, hardware, compute cycles etc.

Threat

Oregon State University
College of Engineering

- Set of circumstances that has the potential to breach security and cause harm
- Example:
  - exposure of customer data
  - corruption of database

Some common threats

Oregon State University
College of Engineering

- Snooping or interception
  - Unauthorized interception of information
- Falsification
  - Unauthorized change of information
- Masquerading or spoofing
  - An impersonation of one entity by another
- Repudiation
  - A false denial of receiving some information or taking an action.

Are all threats/attacks equally important?

Oregon State University
College of Engineering

- Low Impact
  - Limited adverse impact – e.g., loss of time/productivity
- Moderate Impact
  - Serious adverse impact – e.g., some loss of revenue, loss of capability
- High Impact
  - Severe or catastrophic – e.g., potentially bankrupting, loss of life or physical harm

Adversary

Oregon State University
College of Engineering

- Threat agent or an entity that materializes the threat

- Examples:
  - a hackers group that is targeting your customer data

Vulnerability

Oregon State University
College of Engineering

- A weakness in the system that could potentially be exploited to violate security property of interest

- Examples:
  - A misconfiguration or weak security configuration in a computer
  - A bug in the software that could be exploited; like Heartbleed in OpenSSL
  - Weak passwords

Attack

Oregon State University
College of Engineering

- When an entity exploits a vulnerability in a system to violate a security property/attribute

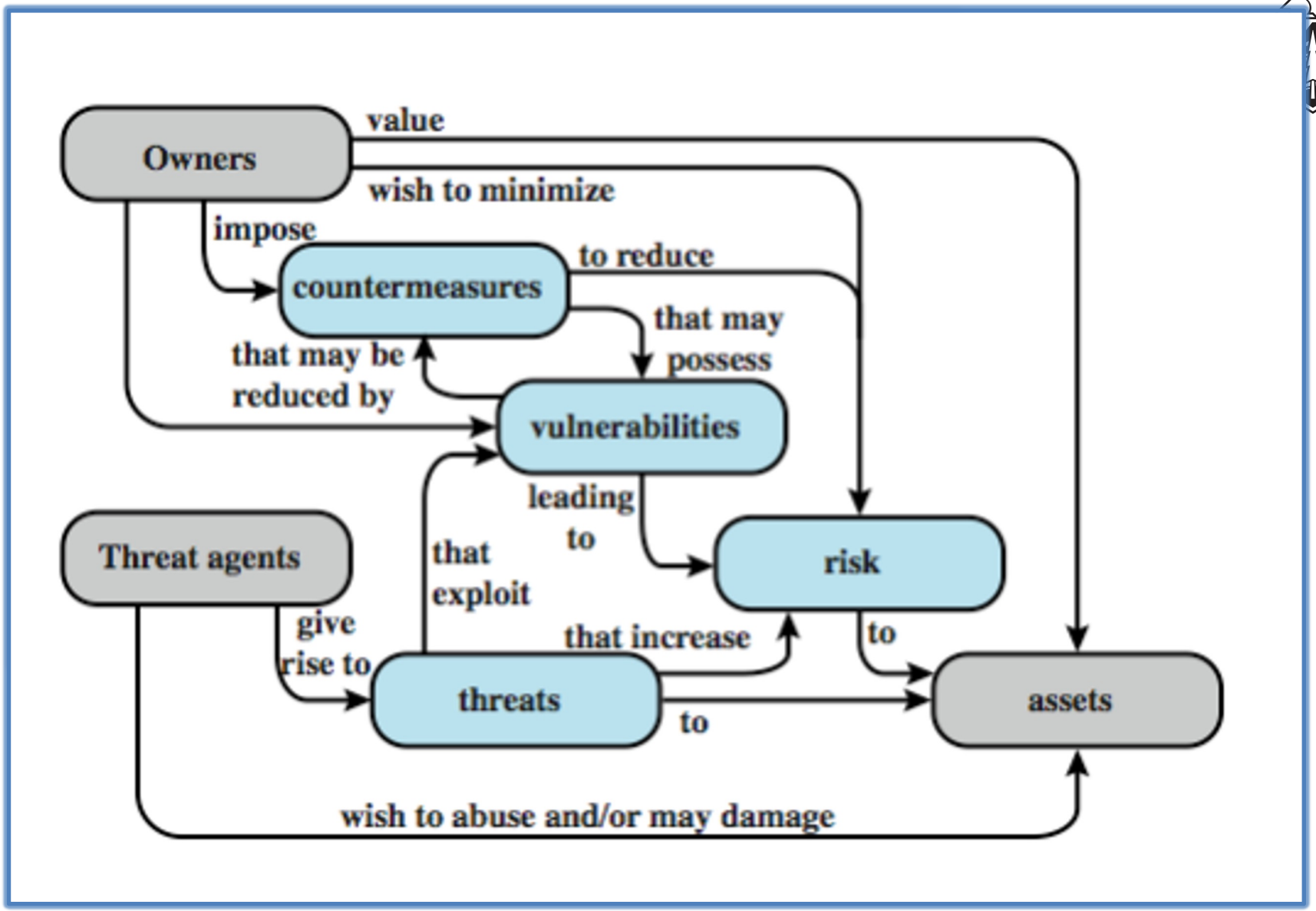
- Examples:
  - an attacker exploits heartbleed bug to steal your cryptographic keys
  - an attacker guesses your weak password to take over your account

Control or Countermeasure

Oregon State University
College of Engineering

- A means or method to
  - prevent a vulnerability from being exploited;
  - or minimize harm from the vulnerability/attack;
  - or detect attack so response and recovery actions may be initiated
  - or respond to or recover from an attack

- Examples:
  - Storing sensitive data encrypted to mitigate the impact of data being stolen
  - An independent data back-up system to prevent loss of data from failures and ransomware attacks



Stallings & Brown

Attack Surface

Oregon State University
College of Engineering

- Is it the sum of vulnerabilities?
- Is it the sum of all exploitable vulnerabilities?
- Reachable exploitable vulnerabilities
  - Network
  - Software
  - Human

Attack Surface Categories

Oregon State University
College of Engineering

Network

- Vulnerabilities accessible over the network
- Include network protocol vulnerabilities

Software

- Vulnerabilities in application, utility, or operating system code
- Web server software in particular

Human

- Social engineering
- Phishing

Summary

Oregon State University
College of Engineering

- We learned the following security terms and relations among them
  - Asset
  - Threat
  - Adversary
  - Vulnerability
  - Controls/Countermeasures
  - Attack Surface

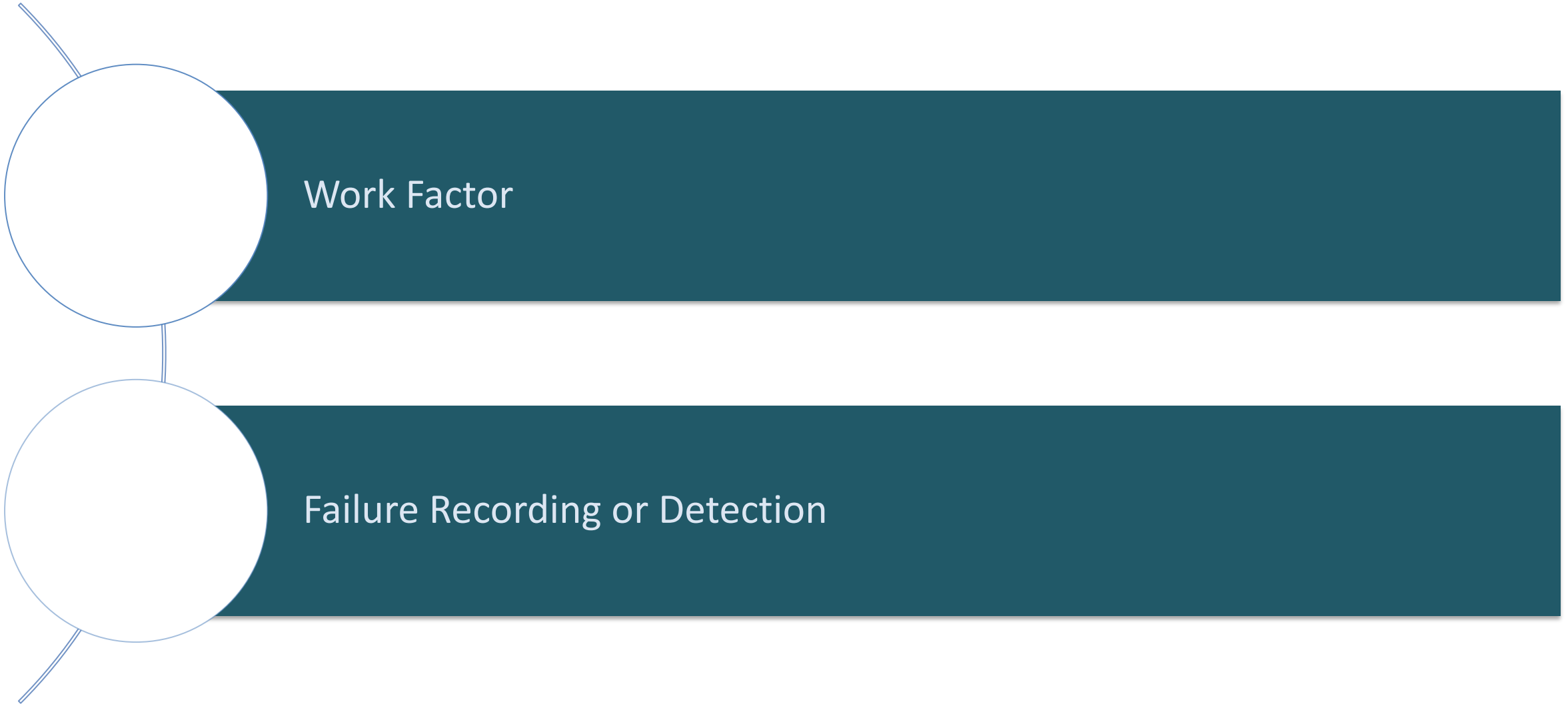
Cyber Security Principles

Security Principles

Oregon State University
College of Engineering

- Economy of Mechanism (Keep it simple)
- Fail-safe (fail-close)
- Complete Mediation
- Open Design
- Separation-of-privilege
- Least-privilege
- Least common mechanism
- Psychological Adoptability (Usability)

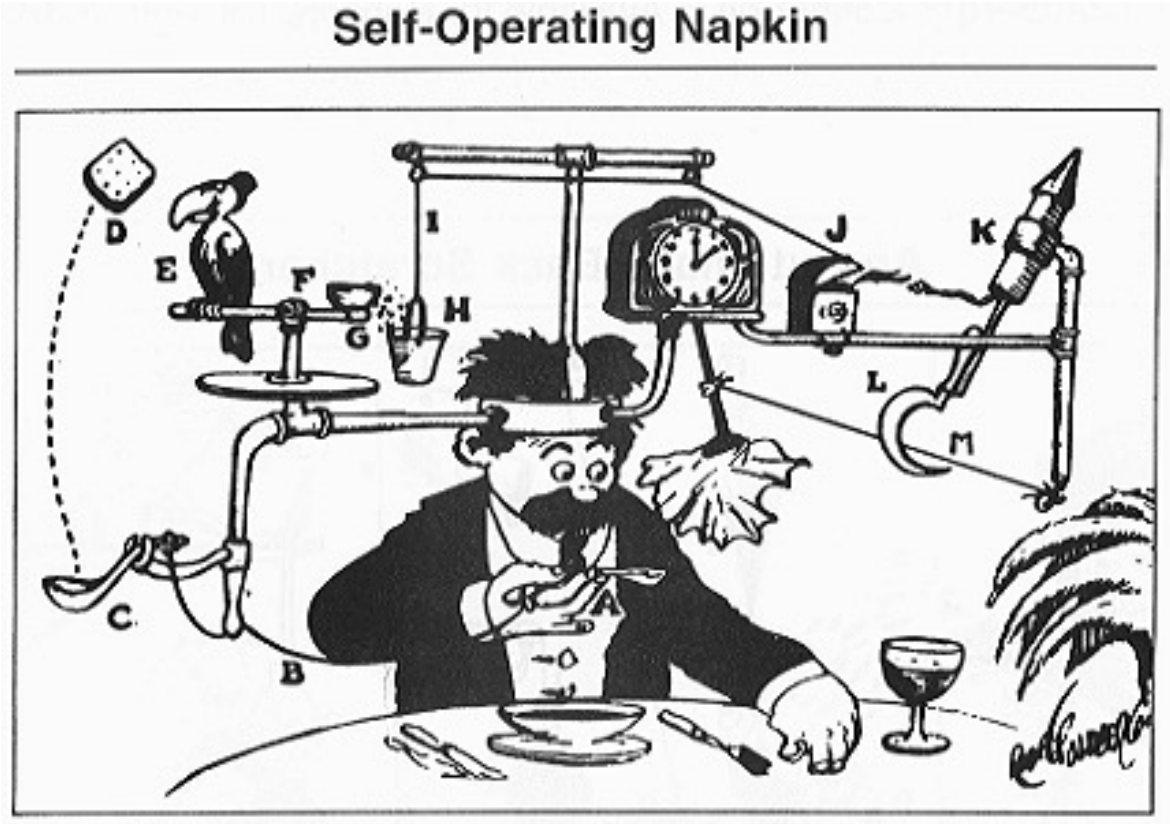
Security Principles



Economy of Mechanism

Oregon State University
College of Engineering

- Keep the design as simple as possible
  - Complex designs will be hard to analyze and verify



Fail-Safe (Fail-Close)

Oregon State University
College of Engineering

- Default should be “no-access”
- Access should be based on explicit permissions
- When a system fails it should default to “no-access”

Complete Mediation

- Every access to every object should be checked for authorization
  - Enforces system-wide view of access control
  - Implies we need a fool-proof (secure) way to identify the source of every request
  - Caching access decisions should be avoided or done with care

Open Design

The security of a design should not depend on the design being secret

Rather, design should be open

Security should depend on only specific information such as cryptographic keys, passwords being secret

Separation-of-Privilege

Oregon State University
College of Engineering

- Critical operations should be protected using two or more {keys, permissions, passwords} that can then be separated (e.g., 2-man rule)
  - One failure or compromise cannot bring down the system

Least Privilege

Oregon State University
College of Engineering

- Every program and every user of the system should operate using the least set of privileges necessary to complete the job
  - Limits the impact/damage of compromise

Least Common Mechanism

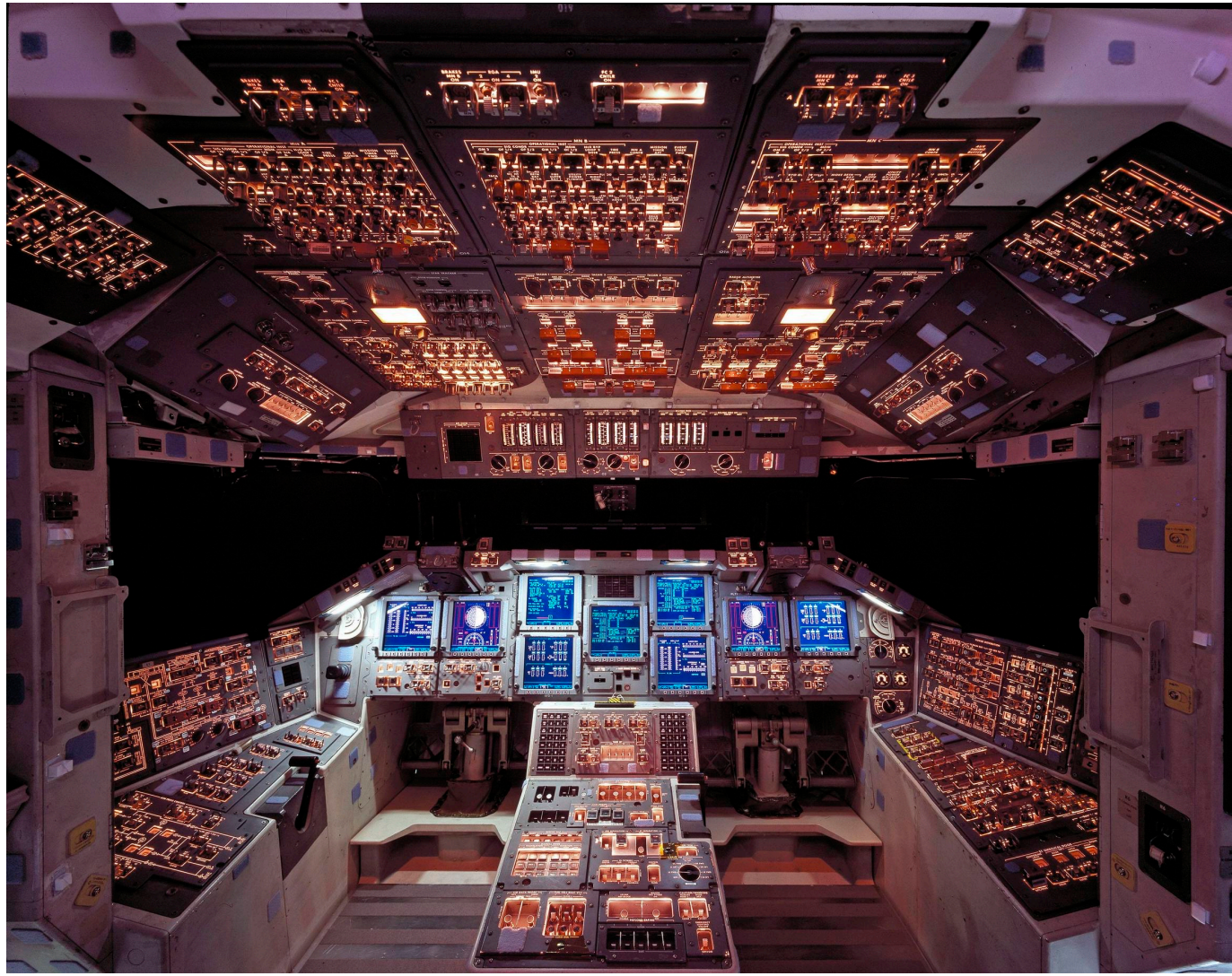
Oregon State University
College of Engineering

- Minimize the amount of mechanism common to more than one user and depended on by all users
  - shared mechanisms (e.g., shared libraries) may provide information paths from one user to another
  - could be a security risk

Psychologial Adoptability (Usability)

Oregon State University
College of Engineering

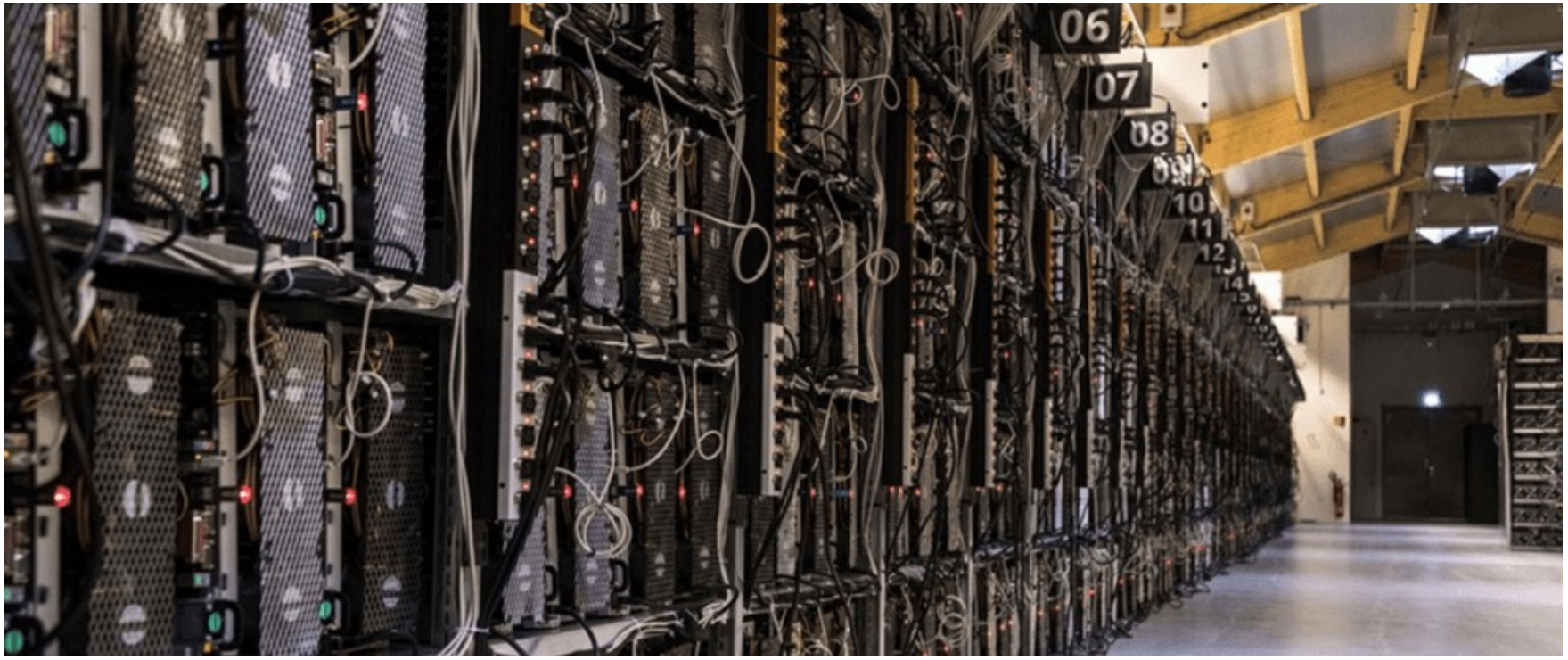
- Essential that human interface be designed for ease of use
  - helps users routinely and automatically apply the protection mechanisms correctly



Work Factor

Oregon State University
College of Engineering

- Compare the cost of circumventing the mechanism with the resources of a potential attacker.



Compromise Recording or Detection

Oregon State University
College of Engineering

- mechanisms that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss
  - argument for detection in place of protection/prevention

Summary

Oregon State University
College of Engineering

- Economy of Mechanism (Keep it simple)
- Fail-safe (fail-close)
- Complete Mediation
- Open Design
- Separation-of-privilege
- Least-privilege
- Least common mechanism
- Psychological acceptability (Usability)
- Work Factor
- Failure Recording or Detection

Cyber Security Strategy

Security Strategy

- Specification/Policy
  - What does it mean to be secured in particular?
- Implementation/Mechanism
  - How to enforce the specified security policy?
- Correctness/Assurance
  - Does the security system work as expected/advertised?
- Incentives
  - Are there right incentives for creating right policy, right mechanisms, and using them?

"You must pinky-swear to never reveal our company secrets. That's the cornerstone of our new information security program."

Specification/Policy

Oregon State University
College of Engineering

- Policy
  - A statement of what is and what is not allowed
  - Divides the world into secure and non-secure states
  - A secure system starts in a secure state. All transitions (changes in system state) keep it in a secure state
- Specification considerations
  - Security vs. ease of use
  - Return on investment – security business case

Is this situation secure?

Oregon State University
College of Engineering

- Web server accepts all connections
  - No authentication required
  - Self-registration
  - Connected to the Internet

Security Mechanism

Oregon State University
College of Engineering

A method, tool, or procedure for enforcing a security policy

- Prevention
  - e.g., encrypting data to preserve confidentiality
- Detection
  - e.g., using integrity checks like crypto hashes to detect tampering
- Response
  - e.g., locking out an account that had too many failed login attempts
- Recovery
  - e.g., backing up data to remote secure storage to recover from data loss

Trust and Assumptions

Oregon State University
College of Engineering

Locks prevent unwanted physical access

What are the assumptions this statement builds on?

Assurance

Oregon State University
College of Engineering

- Evidence of how much to trust a system
- Evidence can include
  - System specifications
  - Design
  - Implementation

Aspirin Assurance Example

Oregon State University
College of Engineering

- Why do you trust Aspirin from a major manufacturer?
  - FDA certifies the aspirin recipe
  - Factory follows manufacturing standards
  - Safety seals on bottles
- Analogy to software assurance

Incentives

Oregon State University
College of Engineering

- Incentives driving the policy
  - what should be allowed and what shouldn't be and why?
- Incentives driving mechanisms
  - should I use passwords or hardware-tokens?
- Incentives driving usage
  - what incentives are there for me to choose a strong password? for not writing it down?
- Incentives driving attackers
  - money? fame? ease of breaking in? fun?

Summary

Oregon State University
College of Engineering

- We examined the four prongs of a good security strategy
  - Security Policy
  - Security Mechanisms
  - Assurance or Correctness
  - Incentives

What is Cryptography

What is Cryptography (1 of 2)

Oregon State University
College of Engineering

Literally…

"Secret Writing"

- Historically focused on encryption
  - Ceaser Cipher is one well-known historical example

What is Cryptography (2 of 2)

Oregon State University
College of Engineering

- Today: much more than secret writing

- Tools & techniques for securing information
  - at rest
  - in transit
  - and even during computations

- A very important piece of security puzzle
  - albeit not a silver bullet

Some Key Cryptographic Tools (1 of 2)

Oregon State University
College of Engineering

- Encryption/Ciphers
  - support Confidentiality and Privacy
  - e.g., AES, 3DES, RSA, ElGamal

- Cryptographic Hashes
  - support Integrity
  - e.g., SHA-256, SHA-512

Some Key Cryptographic Tools (2 of 2)

Oregon State University
College of Engineering

- Message Authentication Codes (MACs)
  - support Integrity
  - e.g., HMAC-SHA256, AES-CBC-MAC

- Digital Signatures
  - support Integrity, Authenticity and Non-repudiation
  - e.g., RSA, DSS

Summary

Oregon State University
College of Engineering

- Cryptography was historically focused on encryption or ‘secret writing’

- Today provides many essential tools beyond encryption for computer and data security

What is Encryption?

What is Encryption? (1 of 3)

Oregon State University
College of Engineering

Encryption primitives or Ciphers are cryptographic primitives used for preserving data confidentiality (and privacy)

What is Encryption? (2 of 3)

Oregon State University
College of Engineering

Encryption transforms ‘plaintext’ (comprehensible) data into ‘ciphertext’ (incomprehensible) data

```
HELLO WORLD ----> KHOOR ZRUOG
```

What is Encryption? (3 of 3)

Oregon State University
College of Engineering

Knowledge of the ‘cryptographic key’ used for the transformation is needed to reverse the transformation

Types of Encryption

Two main types for encryption

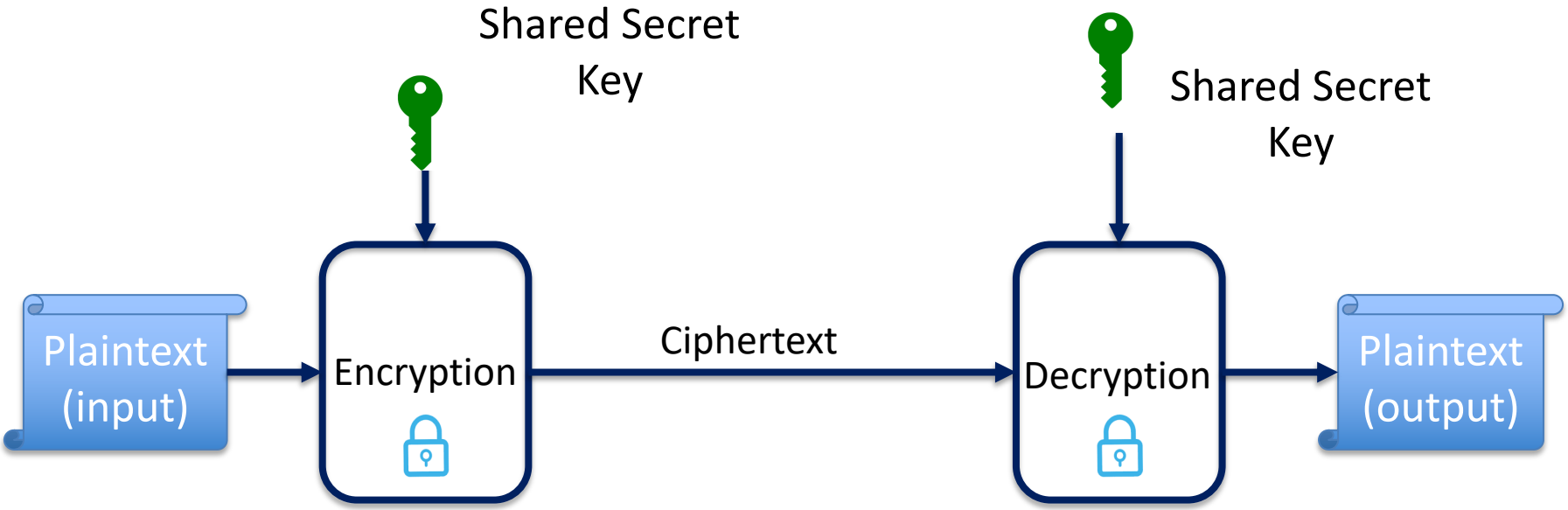
- Symmetric Encryption
  - Key used for enciphering (encryption) and deciphering (decryption) is the same
  - Hence the name symmetric (also called secret-key encryption)
  - Historical (classical) crypto is symmetric

- Asymmetric (or Public-Key) Encryption
  - Keys used for for enciphering (encryption) and deciphering (decryption) are related but different
  - Hence the name asymmetric (also called public-key encryption)
  - Asymmetric crypto is new

Symmetric Encryption

Oregon State University
College of Engineering

- Widely used; commonly called secret-key encryption
- Provides confidentiality
- Five components
  - Plaintext – original message
    - denoted by m
  - encryption algorithm
    - denoted by E
  - Shared secret key
    - denoted by K
  - ciphertext – encrypted message
    - denoted by c; c = E(m,k) or $E_K(M)$ or c = $\{m\}_K$
  - decryption algorithm
    - denoted by D;
- Correctness
  - m = D(E(m,K), K)


Shared Secret Key
Shared Secret Key
Plaintext (input)
Encryption
Ciphertext
Decryption
Plaintext (output)

Public Key Cryptography

Oregon State University
College of Engineering

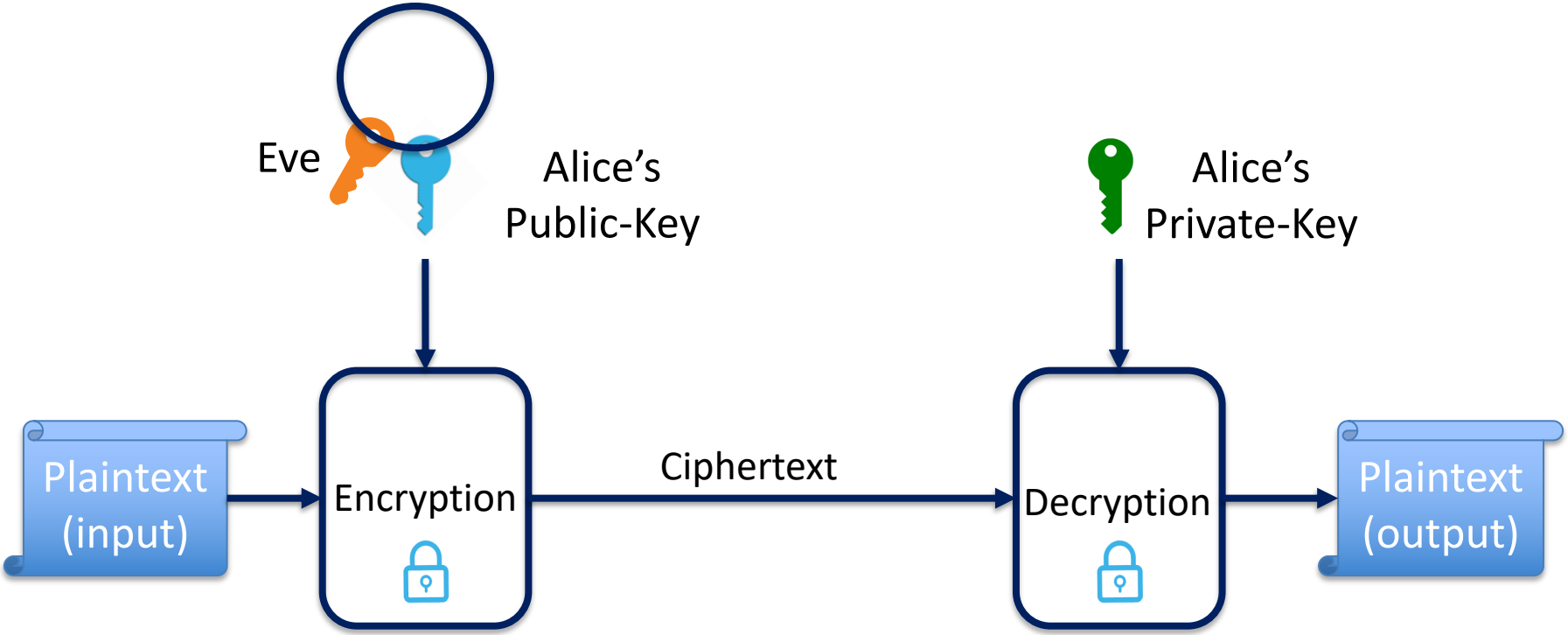
- Two keys
  - *Private key* known only to individual
  - *Public key* available to anyone

- Usage:
  - Confidentiality: encipher using public key, decipher using private key
  - Integrity/authentication: encipher using private key, decipher using public one
  - Symmetric Key distribution

Asymmetric Encryption

Oregon State University
College of Engineering

- Widely used; commonly called public-key encryption
- Provides confidentiality
- Five components
  - Plaintext – original message
    - denoted by m
  - encryption algorithm
    - denoted by E
  - key-pair: public-key, secret-key
    - denoted by (PK, SK)
  - ciphertext – encrypted message
    - denoted by c; c = E(m,PK) or $E_{PK}(M)$ or c = $\{m\}_{PK}$
  - decryption algorithm
    - denoted by D;
- Correctness
  - m = D(E(m,PK),SK)


Eve
Alice's
Public-Key
Alice's
Private-Key
Plaintext
(input)
Encryption
Ciphertext
Decryption
Plaintext
(output)

Attacks on Ciphers [1 of 2]

Oregon State University
College of Engineering

- Opponent whose goal is to break encryption (cryptosystem) is the *adversary*

- Standard cryptographic practice:
  - Assume adversary knows algorithm used, but not the key
  - **Also Known as : Kerckhoffs's principle** or **Shannon's Maxim**

Attacks on Ciphers [2 of 2]

Oregon State University
College of Engineering

Types of attacks

- *ciphertext only*: adversary has only ciphertext; goal is to find plaintext, possibly key
- *known plaintext*: adversary has ciphertext, corresponding plaintext; goal is to find key
- *chosen plaintext*: adversary may supply plaintexts and obtain corresponding ciphertext (access to encryption oracle); goal is to find key
- *chosen ciphertext*: adversary may also supply ciphertexts and obtain corresponding plaintext (access to decryption oracle); goal is to find key

Brute Force Attacks

Oregon State University
College of Engineering

- Systematically checking all keys (pass-phrases) with the hope of eventually finding the right key
  - Also known as exhaustive search

- Example:
  - For *ciphertext only*: given a ciphertext try all possible keys to see if a comprehensible plaintext emerges

  - For *known plaintext:* given a ciphertext and plaintext pair try all possible keys to find the key that decrypts the ciphertext to the plaintext

Basis for Attacks

Oregon State University
College of Engineering

- Mathematical attacks
  - Based on analysis of underlying mathematics

- Statistical attacks
  - Make assumptions about the distribution of letters, pairs of letters (diagrams), triplets of letters (trigrams), *etc.*
    - Called *models of the language*
  - Examine ciphertext, correlate properties with the assumptions

Summary

- Encryption transforms plaintext (comprehensible) into ciphertext (not comprehensible without the key)
- Two types of Encryption
  - Symmetric: same key for encryption and decryption
  - Asymmetric: different key for encryption and decryption
- Symmetric encryption has been around a long time
  - At least since the time of Caesar
- Asymmetric encryption is newer (publicly known since late 70's)
- Adversaries can try to break an encryption system
  - try to guess the plaintext by looking at the ciphertext
  - or guess the key after looking at one or more (plaintext, ciphertext) pairs

Classical Ciphers

Classical Ciphers [1 of 3]

Oregon State University
College of Engineering

- Encryption or ciphers have been around for a long time
  - At least since Caesar's time
  - Caesar Cipher is a well-known historical example

Classical Ciphers [2 of 3]

Oregon State University
College of Engineering

- Classical ciphers are ***symmetric***
  - Sender, receiver share common key
  - Keys may be the same, or trivial to derive from one another

- Two basic types
  - *Transposition* ciphers
  - *Substitution* ciphers
  - Combinations are called *product ciphers*

Classical Ciphers [3 of 3]

Oregon State University
College of Engineering

- Transposition Ciphers
  - Permute the symbols (characters) in the message
  - Examples: Rail cipher, n-transpositional cipher, scytale
- Substitution Ciphers
  - Substitute the symbols (characters) in the message
  - Examples: Cæsar cipher, One Time Pad, Book cipher

Transposition Cipher [1 of 3]

Oregon State University
College of Engineering

- Plaintext and Ciphertext use the same alphabet
- Scramble letters in plaintext to produce ciphertext

- Example (Rail-Fence)
  - Plaintext is `HELLO WORLD`
  - Write the plaintext on alternating "rails"
    - »H E
    - »L L
    - »O W
    - »O R
    - »L D
  - Ciphertext is `HLOOLELWRD`

Transposition Cipher [1 of 2]

Oregon State University
College of Engineering

- Generalize to n-columnar transpositions
- Write text in fixed length rows.
- Read ciphertext out in column major order

```
H E L
L O W
O R L
D X X
HLODEORXLWLX
```

  - Could also permute the columns

Transposition Ciphers [1 of 3]

Oregon State University
College of Engineering

- What is the key in Rail-Fence or n-columnar transposition?

Other Transposition Ciphers

- Scytale (older than 300BC in Greece!)

Columnar Transposition

- # of columns and order of columns is encoded by a key
  - Ex: “WORD” ⇒ 4 columns and rearranged in the order 4, 2, 3, 1
    - W is 4th alphabetically in the key
    - 0 is 2nd alphabetically in the key...

Double Columnar Transposition

- Apply Columnar Transposition twice
  - Can use two different passwords

Double Columnar Transposition

Oregon State University
College of Engineering

- Apply Columnar Transposition twice
  - Can use two different passwords

- Used in WWI US Military

Double Columnar Transposition

Oregon State University
College of Engineering

- Apply Columnar Transposition twice
  - Can use two different passwords
- Used by US Military in WW-I
- Ubchi -- a variation used by Germany in WW-I
  - Same password twice
  - different padding

Substitution Ciphers [1 of 2]

Oregon State University
College of Engineering

- Change characters in plaintext to produce ciphertext

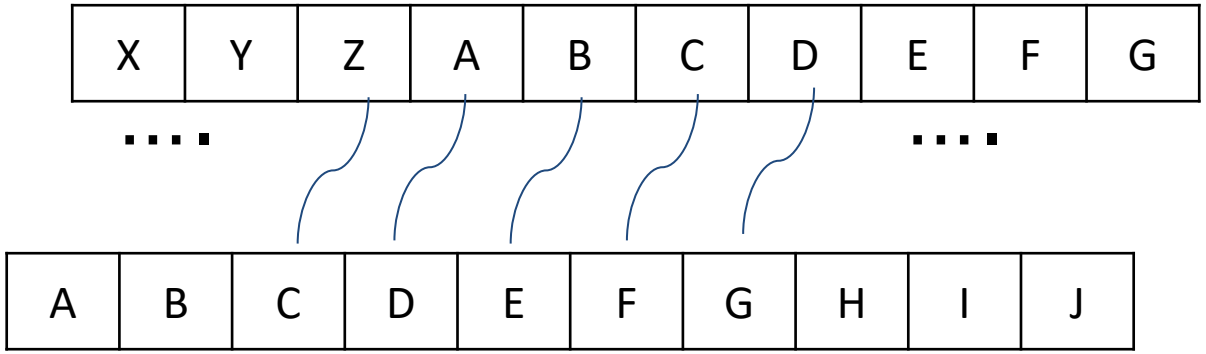
- Example (Cæsar cipher)
  - Plaintext is `HELLO WORLD`
  - Change each letter to the third letter following it (A goes to D, X goes to A, Y to B, Z to C)
  - Ciphertext is `KHOOR ZRUOG`

Caesar Cipher

Oregon State University
College of Engineering

Reportedly used by Julius Caesar

- It is a shift cipher with a shift of 3 (A → D)



Caesar Cipher

Plaintext: Hello World

H → K, E → H, L → O, O → R

⇒ Hello → Khoor

W → Z, O → R, R → U, L → O, D → G

⇒ World → Zruog

Caesar Cipher

Oregon State University
College of Engineering

It is a Substitution Cipher:

Plaintext Alphabet:

A	B	C	D	E	F	G	H	I	J	…

Ciphertext Alphabet:

D	E	F	G	H	I	J	K	L	M	…

Keys in Ciphers

Oregon State University
College of Engineering

- What is the “key” for Caesar Cipher?

Caesar Cipher Exercise

Oregon State University
College of Engineering

http://rumkin.com/tools/cipher/

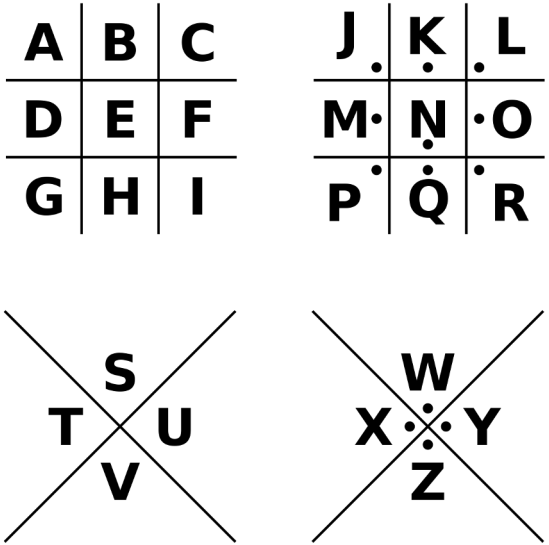
Decode

Fdhvhu Vkliw Lv Grsh

Other Substitution Ciphers

Oregon State University
College of Engineering

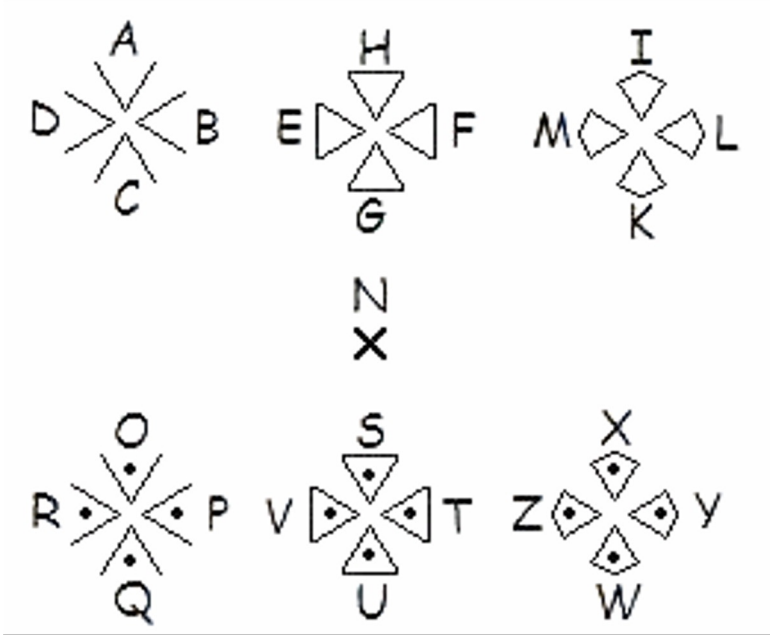
- Pigpen (Masonic or Tic-Tac-Toe) Cipher



Other Substitution Ciphers

Oregon State University
College of Engineering

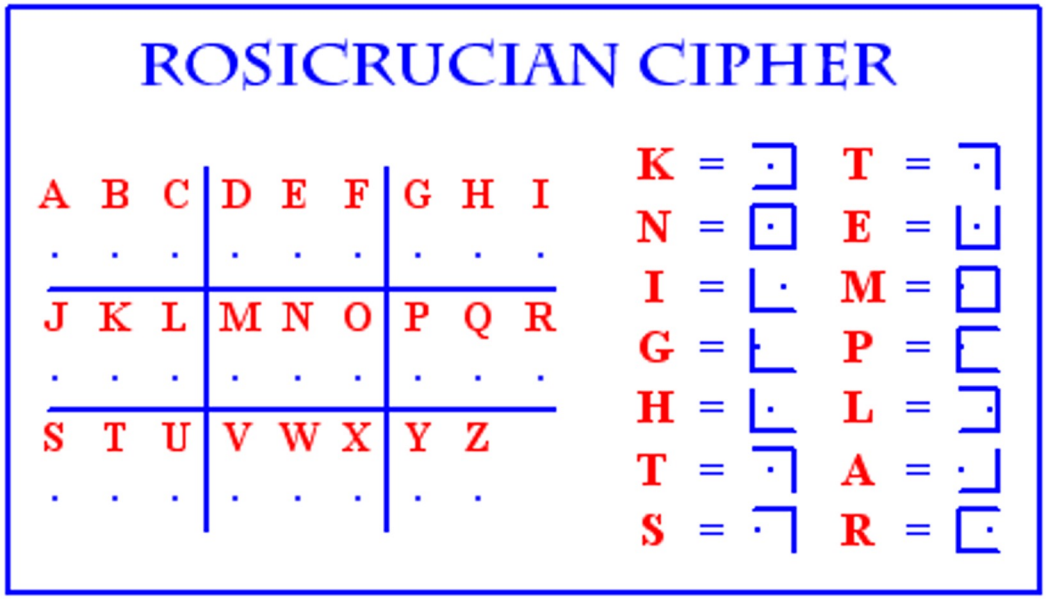
- Templar Cipher



Other Substitution Ciphers

Oregon State University
College of Engineering

- Rosicrucian Cipher



Keys in Ciphers

- What is the “key” for Tic-Tac-Toe Cipher?

Other Substitution Ciphers

- Caesar Cipher is "*monoalphabetic*"
  - *one* substitution alphabet
- What if we can combine two alphabets?
  - Ex: one substitution alphabet for odd letters and a different alphabet for one for even letters?
- What if we can use more than two!
  - we get "*polyalphabetic*" ciphers

Polyalphabetic Ciphers

Vigenere Cipher

- Key has multiple letters
  - Ex: "*paswd*"
    - Contrast with Caesar (Key is "*d*")

Polyalphabetic Ciphers

Vigenere Cipher

- Key has multiple letters
  - Ex: "*paswd*"
    - Contrast with Caesar (Key is "*d*")

- `Hello World` with key "`paswd`"
  - Try it on Rumkin!

Polyalphabetic Ciphers

Vigenere Cipher

- Key has multiple letters
  - Ex: "*paswd*"
    - Contrast with Caesar (Key is "*d*")

- `Hello World` with key "`paswd`"
  - Try it on Rumkin!
    - `Wedhr Lojhg`

Cryptanalysis

- Both Ceasar and n-columnar are easily breakable!

- Example: breaking Ceasar Cipher
  - Brute Force: try all possible (26) keys
  - Statistical: look at letter frequencies
    - "E" is the most common letter in English language
    - most common letter in ciphertext likely corresponds to "E"

Cryptanalysis - Breaking Ciphers!

Oregon State University
College of Engineering

Abu Yusuf Al Kindi, Arab mathematician, philosopher from 9th century AD is credited with discovering *frequency analysis*

One-Time Pad

Oregon State University
College of Engineering

- A cipher with a random key at least as long as the message
  - Provably unbreakable!!
  - Why?

- Let us consider a one-time pad scheme that uses Caeser Cipher

One-Time Pad

Oregon State University
College of Engineering

- Look at ciphertext `DXQR`.
- Equally likely to correspond to plaintext `DOIT` (key `AJIY`) and to plaintext `DONT` (key `AJDY`) and any other 4 letters

- Warning: keys *must* be random, or you can attack the cipher by trying to regenerate the key
  - Approximations, such as using pseudorandom number generators to generate keys, are *not* random

Book Cipher

Oregon State University
College of Engineering

- Approximate one-time pad with book text
  - Sender and receiver agree on text to pull key from
  - Bible, Koran, Phone Book
- Problem is that book text is not random
  - Combine English with English
  - Can still perform language based statistical analysis

Summary

Oregon State University
College of Engineering

- Classic ciphers are symmetric
- They are either transposition (or permutation ciphers), substitution ciphers, or product ciphers (combination)
- These pen and paper classical ciphers have been used historically
- Not practical in the age of the computer – easy to break
- The components (transposition and substitution) are the same in modern ciphers
- One-time pad is provably unbreakable!