UCS1505 INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES

Presentation by:
Dr. V. Balasubramanian
SSN College of Engineering

Course Objectives

- To understand the classical and symmetric cryptographic techniques
- To study about message authentication and hash functions
- To learn number theory fundamentals needed by cryptographic algorithms
- To understand the various key distribution and management schemes
- To understand the concepts of Public key cryptography and digital signatures.

Course Outcome

- On successful completion of this course, the student will be able to:
- Describe and implement classical and symmetric ciphers (K2)
- Describe the authentication schemes and hash algorithms (K2)
- Understand the number theoretic foundations of cryptography (K3)
- Compare and contrast various Public key cryptographic techniques (K3)
- Illustrate various Public key cryptographic techniques (K3).

History of Cryptography

hieroglyphs - around 2000 B.C.

漢字 汉字

ideogram - ancient Chinese

Clay tablets from Mesopotamia

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

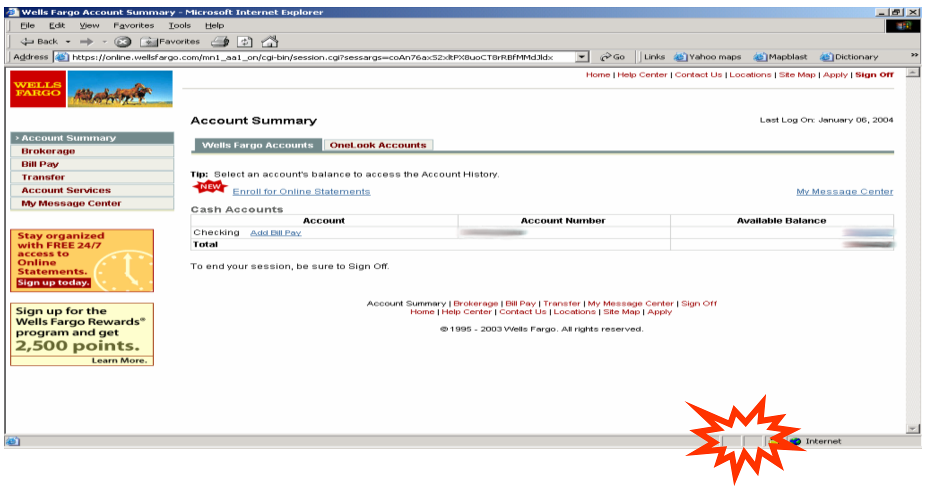
Atbash cipher - around 500 to 600 BC

Scytale - Spartan

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

Polybius Square - Greek method

Secure communication



HTTPS

no eavesdropping
no tampering

Secure Sockets Layer / TLS

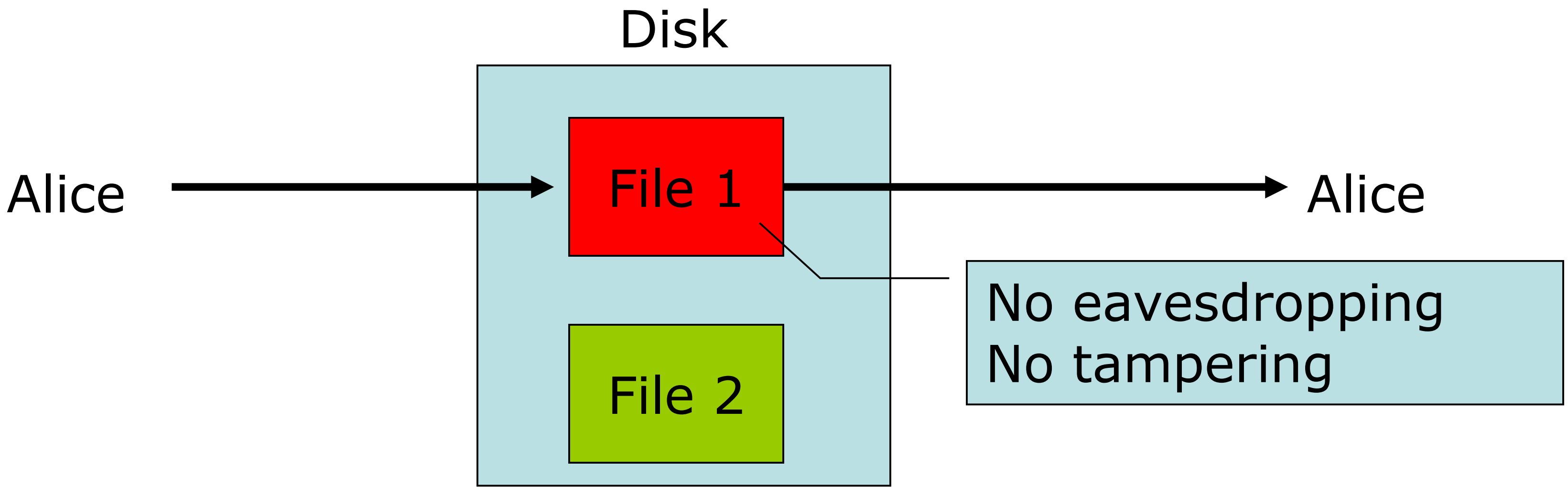
Two main parts

1. Handshake Protocol: **Establish shared secret key using public-key cryptography** (2nd part of course)

2. Record Layer: **Transmit data using shared secret key**

   Ensure confidentiality and integrity (1st part of course)

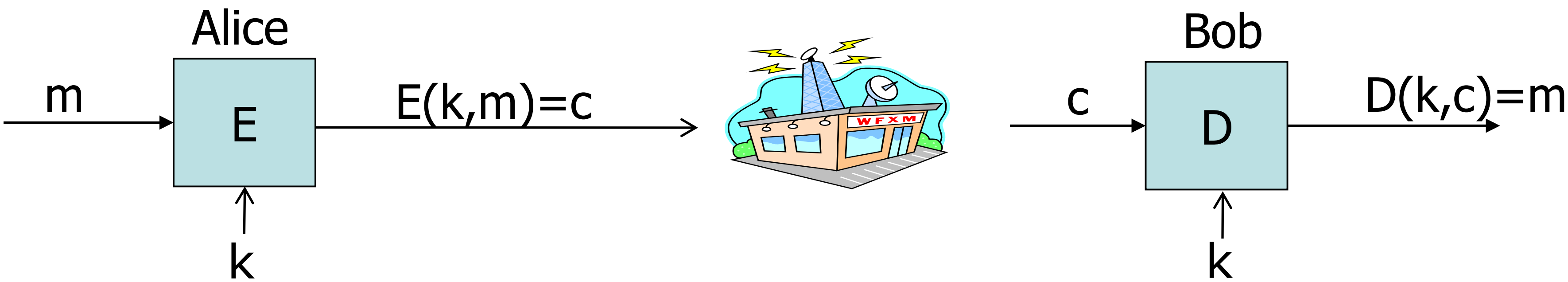
Protected files on disk



Analogous to secure communication:

Alice today sends a message to Alice tomorrow

Building block: sym. encryption



E, D: cipher k: secret key (e.g. 128 bits)
m, c: plaintext, ciphertext

Encryption algorithm is publicly known

- Never use a proprietary cipher

Things to remember

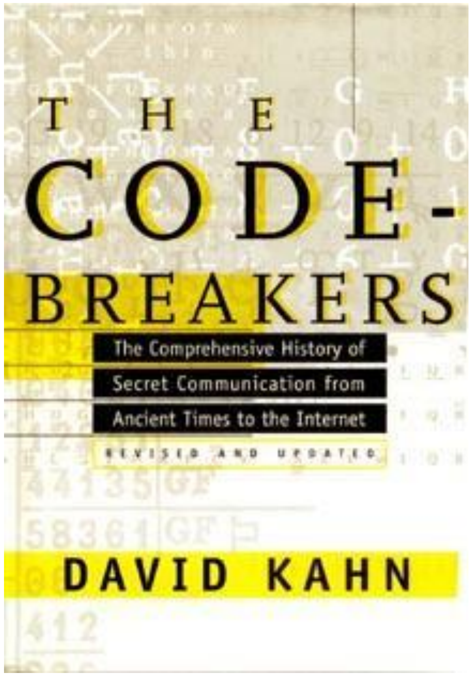
Cryptography is:

- A tremendous tool
- The basis for many security mechanisms

Cryptography is not:

- The solution to all security problems
- Reliable unless implemented and used properly
- Something you should try to invent yourself
  - many many examples of broken ad-hoc designs

- David Kahn, “The code breakers” (1996)



Price Water Cooper

Increased Security Breaches

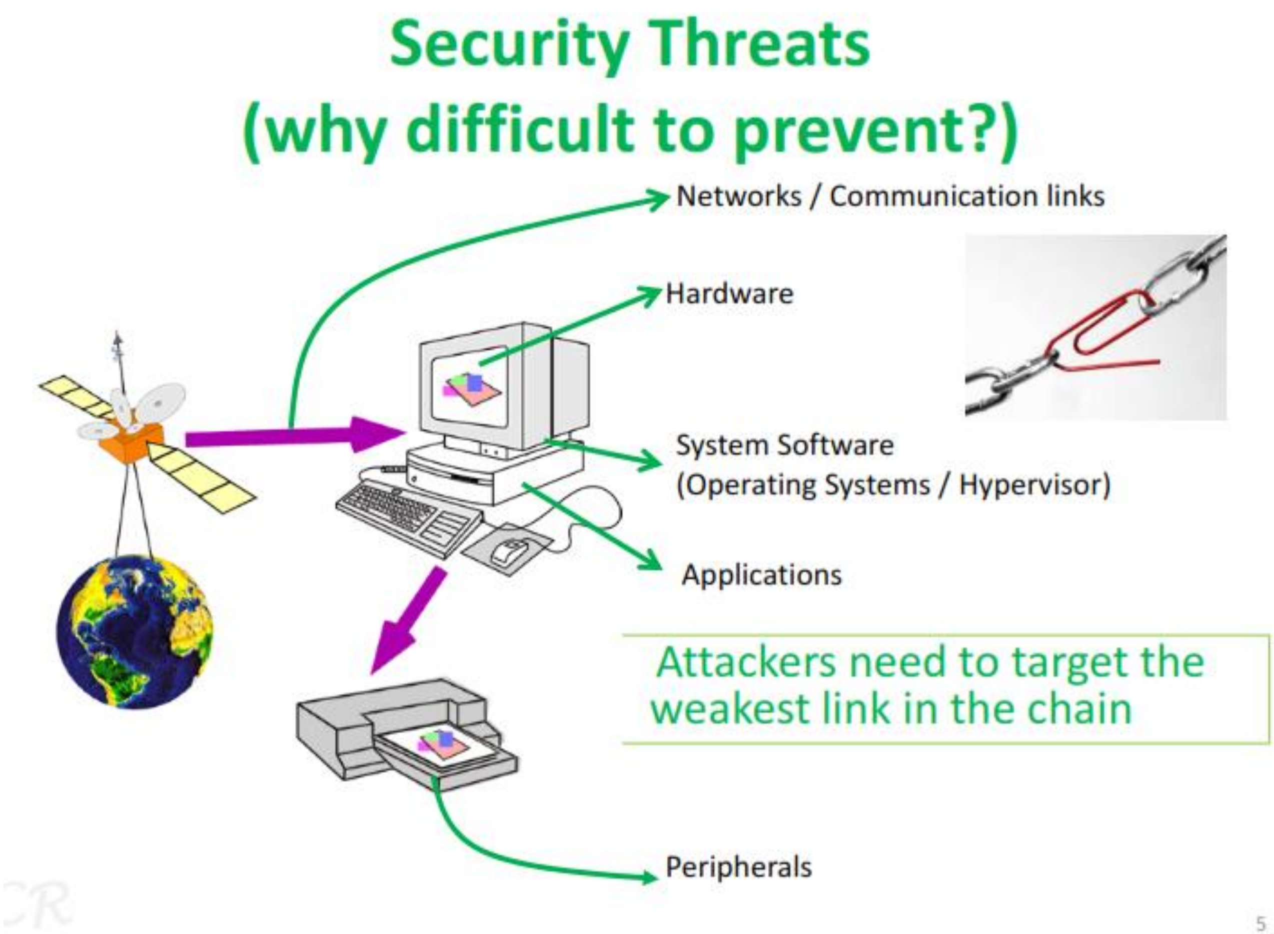
81% more in 2015

90% of large organisations
74% of small businesses
had a security breach.
▲ Up from 81% a year ago.
▲ Up from 60% a year ago.

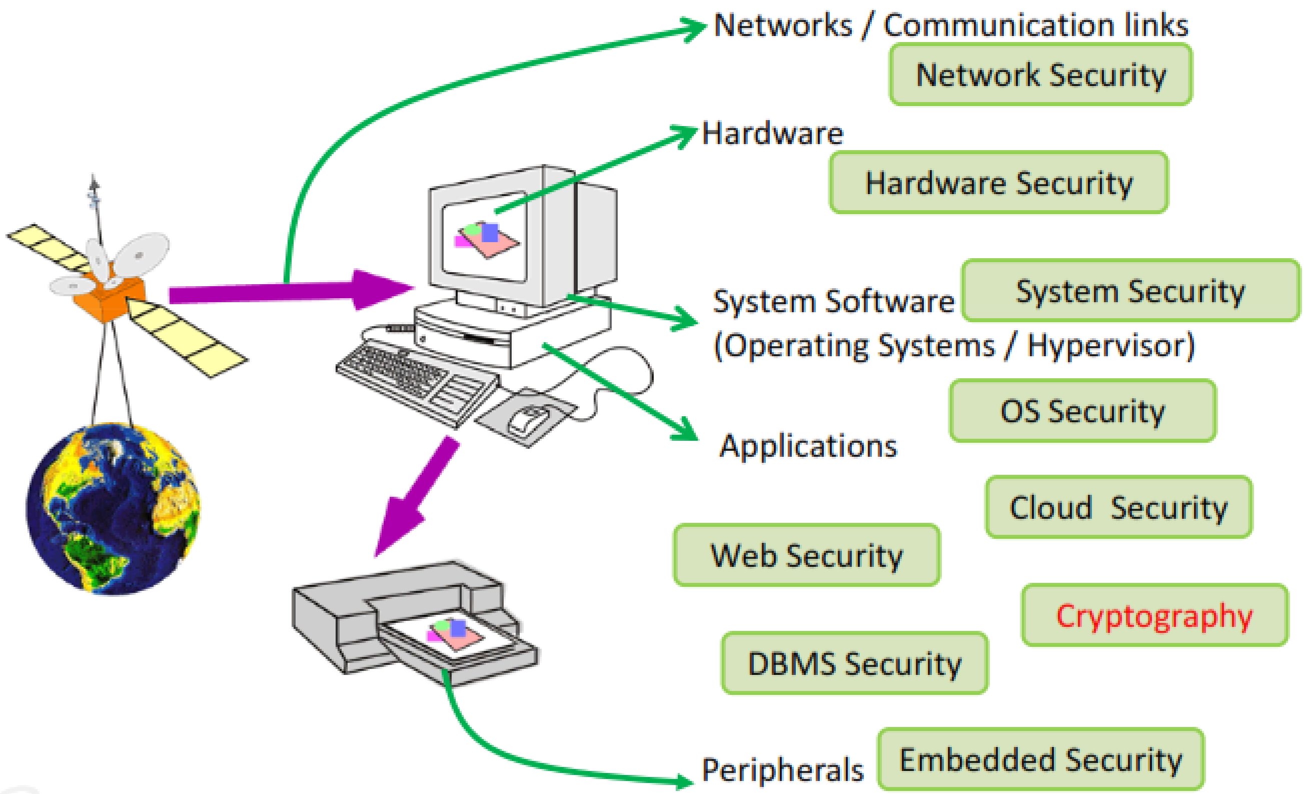
£1.46m - £3.14m is the average cost to a large organisation	**£75k - £311k** is the average cost to a small business

44% of large organisations
44% of small businesses
increased information security spend in the last year.

Security Threats

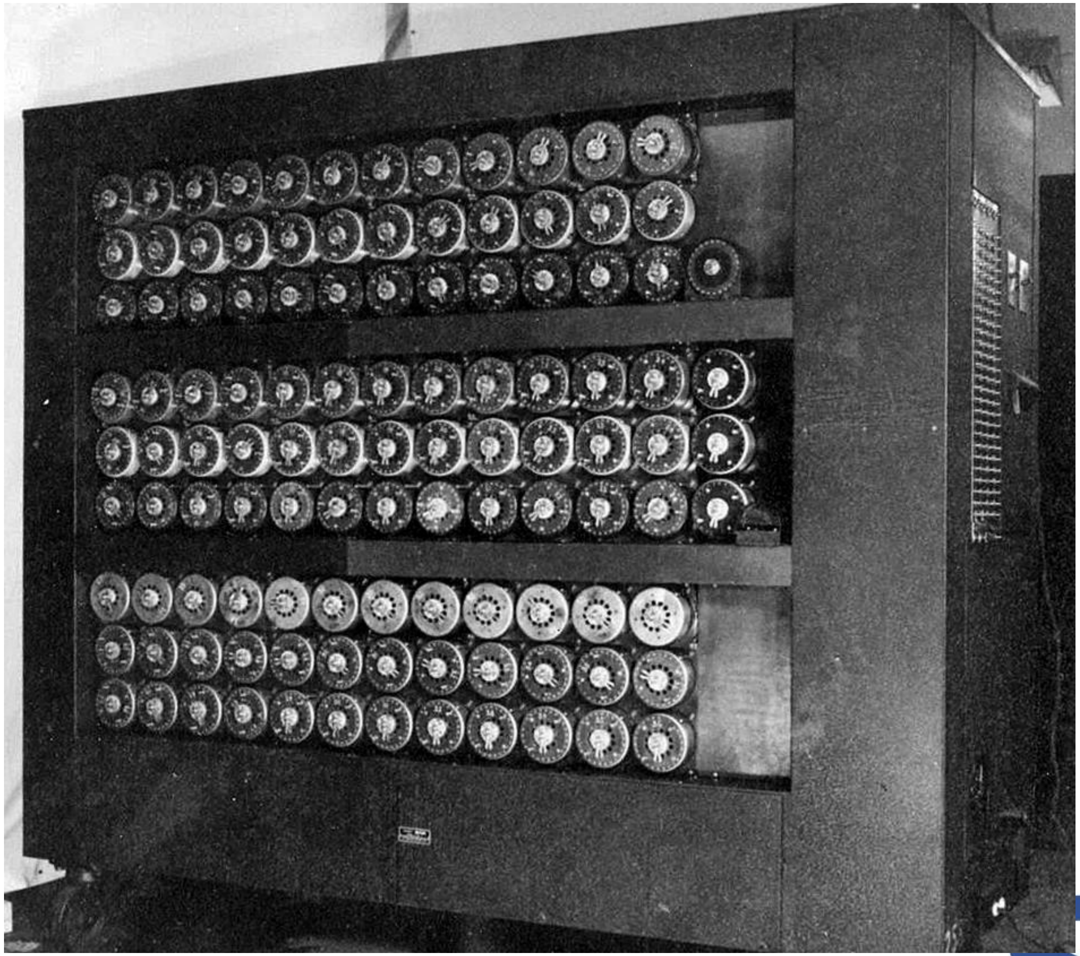


Security Study



Enigma

Bombe



Turing Award

Increased Security Breaches (PWC)

81% more in 2015

90% of large organisations

74% of small businesses

had a security breach.

▲ Up from 81% a year ago.

▲ Up from 60% a year ago.

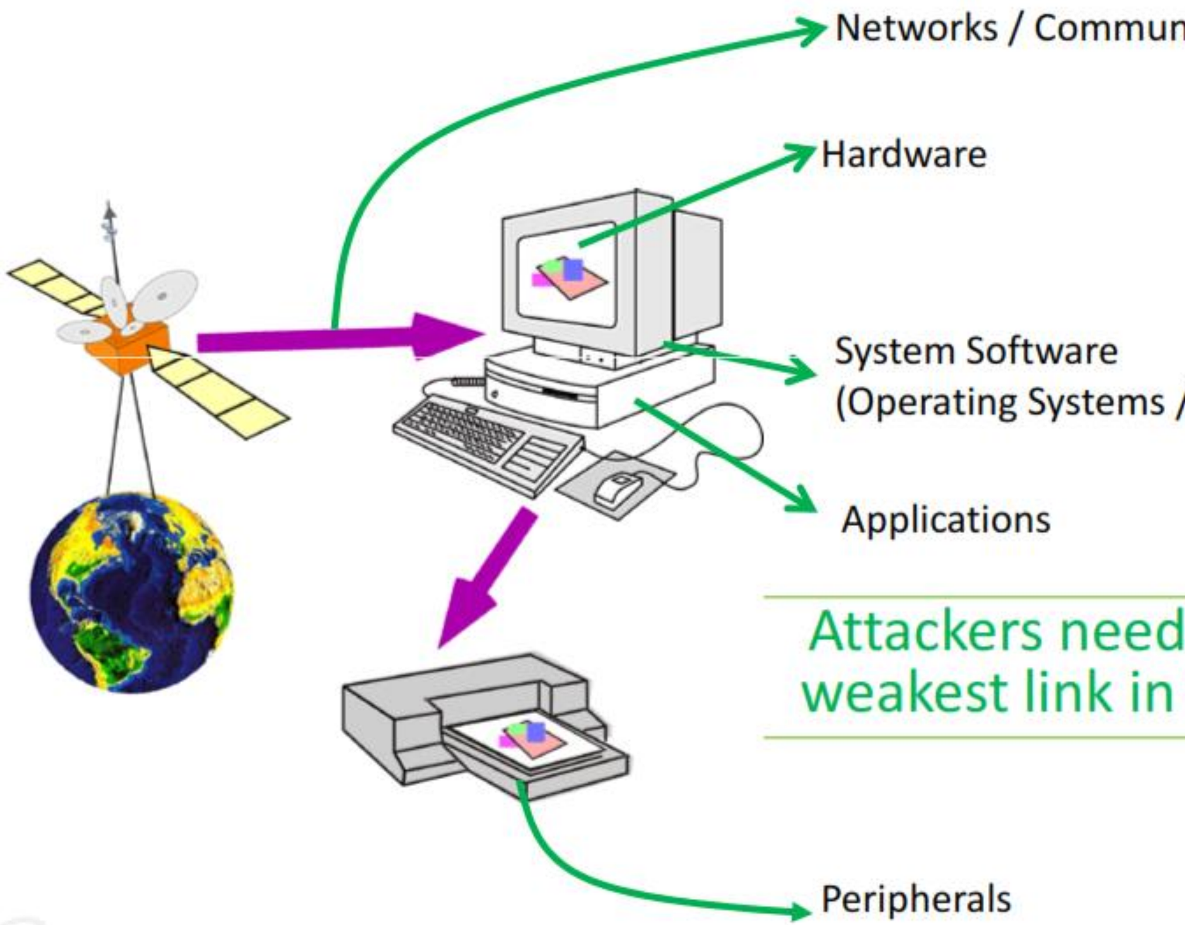
£1.46m - £3.14m is the average cost to a large organisation	**£75k - £311k** is the average cost to a small business

44% of large organisations

44% of small businesses

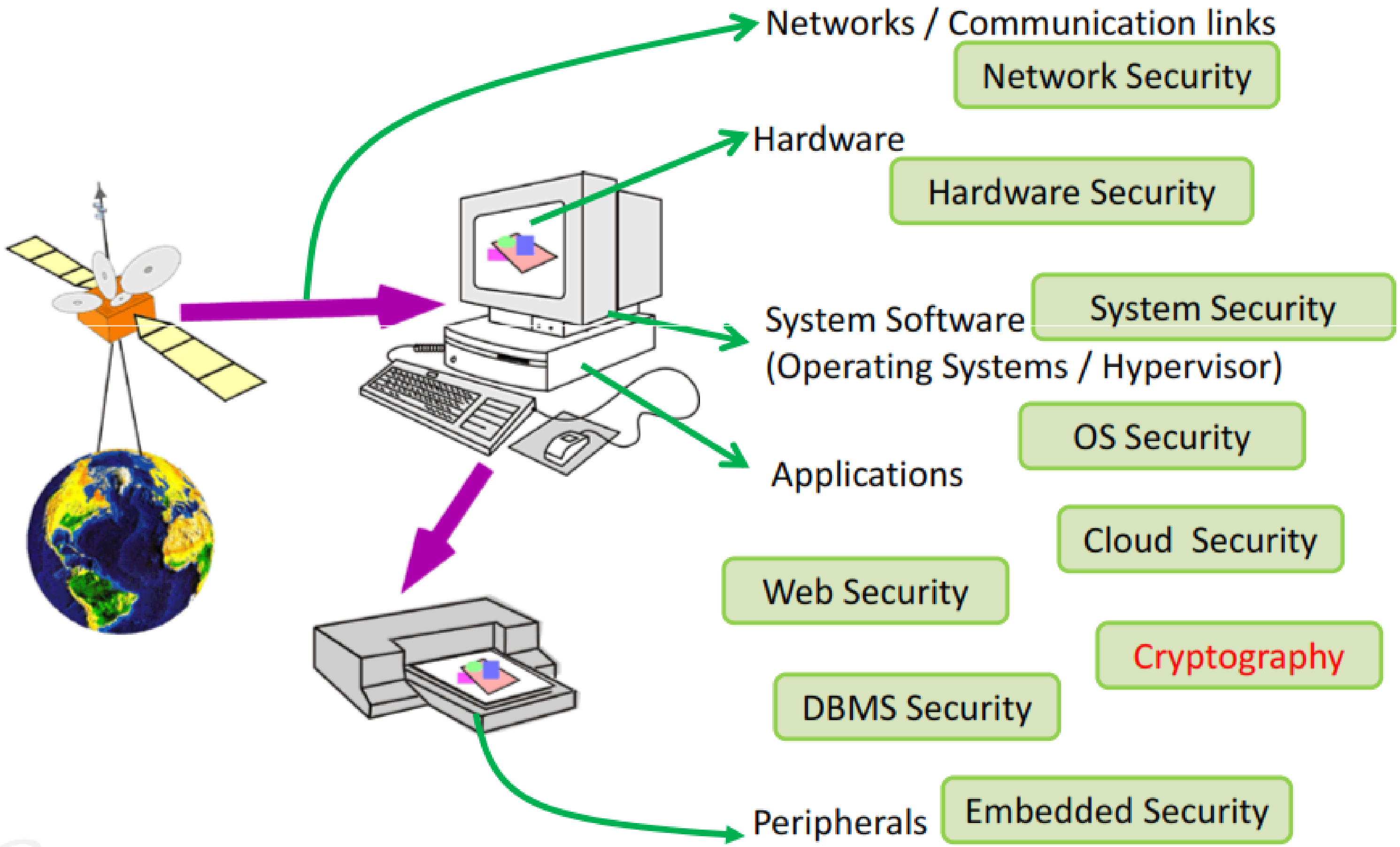
increased information security spend in the last year.

Security Threats



Attackers need to target the weakest link in the chain

Security Studies



Cryptography (historically)

"...the art of writing or solving codes…"

- Historically, cryptography focused exclusively on ensuring *private communication* between two parties sharing secret information in advance (using "codes" aka *private-key encryption*)

Modern cryptography

- Much broader scope!
  - Data integrity, authentication, protocols, …
  - The *public-key setting*
  - Group communication
  - More-complicated trust models
  - Foundations (e.g., number theory, quantum-resistance) to systems (e.g., electronic voting, cryptocurrencies)

Modern cryptography

Design, analysis, and implementation of ***mathematical techniques*** *for securing information, systems, and distributed computations against adversarial attack*

Modern cryptography

- Cryptography is ubiquitous
  - Passwords, password hashing
  - Secure credit-card transactions over the internet
  - Encrypted WiFi
  - Disk encryption
  - Digitally signed software updates
  - Bitcoin
  - …

Cryptography (historically)

"…the art of writing or solving codes…"

- Historically, cryptography was an *art*
  - Heuristic, unprincipled design and analysis
  - Schemes proposed, broken, repeat…

Modern cryptography

- Cryptography is now much more of a *science*
  - Rigorous analysis, firm foundations, deeper understanding, rich theory
- The “crypto mindset” has permeated other areas of computer security
  - Threat modeling
  - Proofs of security

Rough course outline

	Secrecy	**Integrity**
Private-key setting	Private-key encryption	Message authentication codes
Public-key setting	Public-key encryption	Digital signatures

- Building blocks
  - Pseudorandom (number) generators
  - Pseudorandom functions/block ciphers
  - Hash functions
  - Number theory

Cryptography

- A crucial component in all security systems
- Fundamental component to achieve
  - Confidentiality
  - Data Integrity
  - **Authentication**
  - Non-Repudiation

Cryptography helps prove identities

Classical Cryptography

Motivation

- Allows us to “ease into things…,” introduce notation
- Shows why unprincipled approaches are dangerous
- Illustrates why things are more difficult than they may appear

Classical cryptography

- Until the 1970s, exclusively concerned with ensuring *secrecy* of communication
- i.e., *encryption*

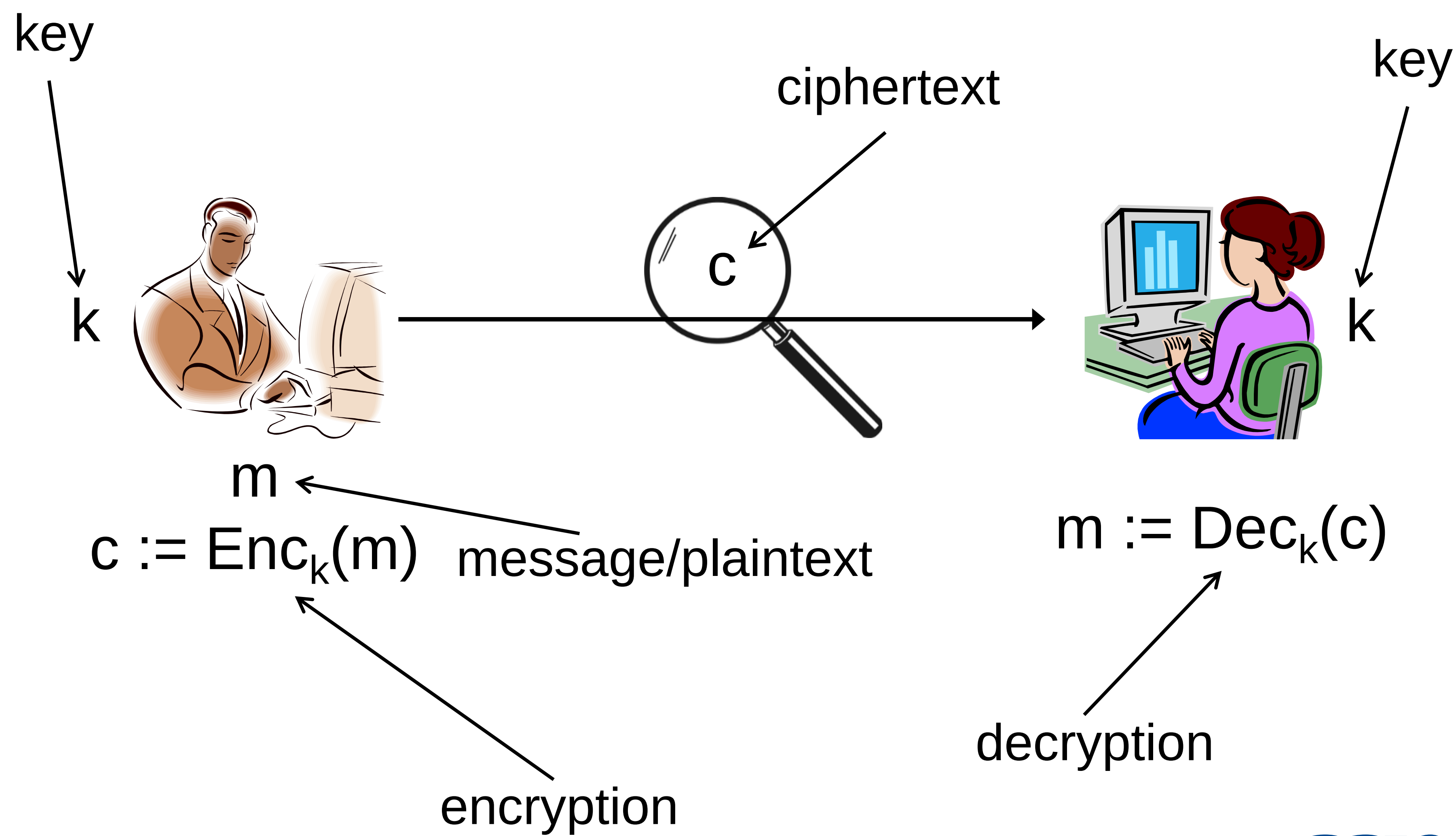
Classical Cryptography

- Until the 1970s, relied exclusively on secret information (a *key*) shared in advance between the communicating parties

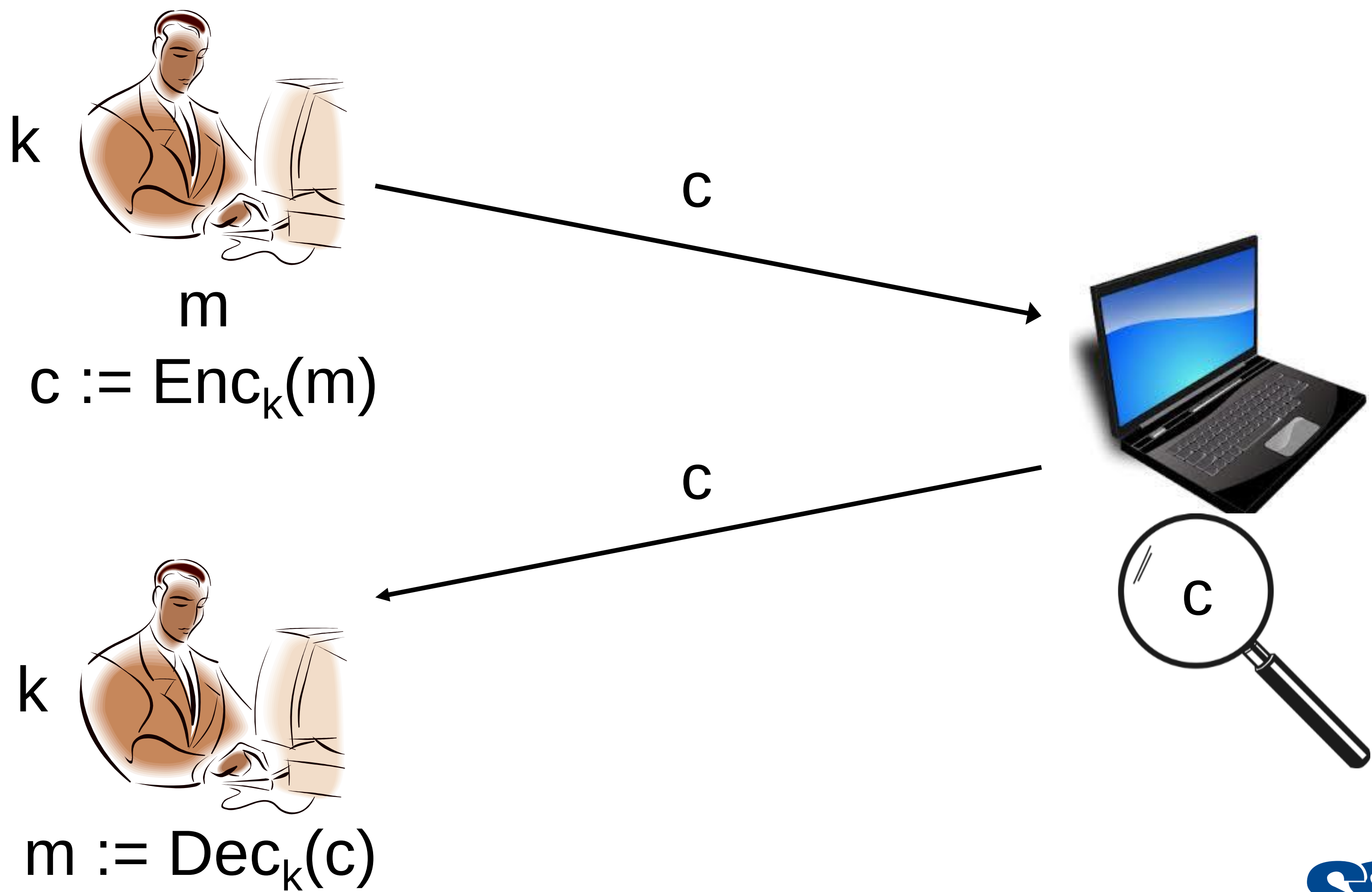
Private-key cryptography

- – aka secret-key / shared-key / symmetric-key cryptography ssn

Private-key encryption



Private-key encryption



Private-key encryption

- A *private-key encryption scheme* is defined by a message space $\mathcal{M}$ and algorithms (Gen, Enc, Dec):
  - Gen (key-generation algorithm): outputs $k \in \mathcal{K}$
  - Enc (encryption algorithm): takes key k and message $m \in \mathcal{M}$ as input; outputs ciphertext c
    $$c \leftarrow Enc_k(m)$$
  - Dec (decryption algorithm): takes key k and ciphertext c as input; outputs m or "error"

For all $m \in \mathcal{M}$ and k output by Gen,

$$Dec_k(Enc_k(m)) = m$$

Kerckhoffs's principle

- *The encryption scheme* is not secret
  - The attacker knows the encryption scheme
  - The only secret is the *key*
  - The key must be chosen at random; kept secret

- Some arguments in favor of this principle
  - Easier to keep *key* secret than *algorithm*
  - Easier to change *key* than to change *algorithm*
  - Standardization
    - Ease of deployment
    - Public validation

The shift cipher

- Consider encrypting English text
- Associate ‘a’ with 0; ‘b’ with 1; …; ‘z’ with 25
  - $k \in \mathcal{K} = \{0, \ldots, 25\}$

```
helloworldz
ccccccccccc
-----------
jgnnqyqtnfb
```

- To encrypt using key k, shift every letter of the plaintext by k positions (with wraparound)
- Decryption just does the reverse

Substitution Technique

- Is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- Simplest and earliest known use of a substitution cipher
- Used by Julius Caesar
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher Algorithm

- Can define transformation as:

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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Mathematically give each letter a number

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Algorithm can be expressed as:

$$c = \mathrm{E}(3, p) = (p + 3) \bmod (26)$$

  - A shift may be of any amount, so that the general Caesar algorithm is:

$$C = E(k , p) = (p + k) \bmod 26$$

- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

$$p = D(k , C) = (C - k) \bmod 26$$