Introduction to Cryptography and Network security

Course Objectives

- The student should be made to:
- Understand OSI security architecture and classical encryption techniques.
- Acquire fundamental knowledge on the concepts of finite fields and number theory.
- Understand various block cipher and stream cipher models.
- Describe the principles of public key cryptosystems, hash functions and digital signature.

Course Outcome

Upon Completion of the course, the students should be able to:

- Compare various Cryptographic Techniques
- Design Secure applications
- Inject secure coding in the developed applications

Cryptography (common tool to protect data) is everywhere

Secure communication:

- web traffic: HTTPS
- wireless traffic: 802.11i WPA2 (and WEP, WiFi protected accessv), GSM, Bluetooth

Encrypting files on disk: EFS Encrypting File System, TrueCrypt(on the fly encryption)

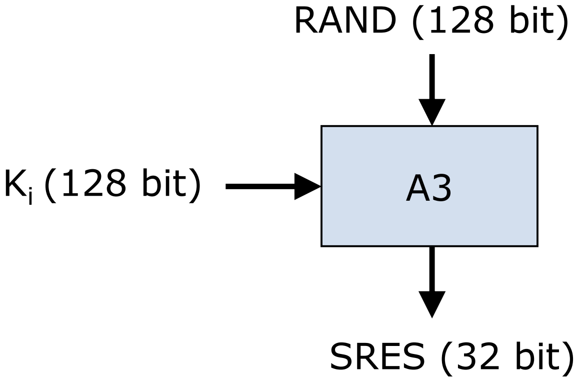
Content protection (e.g. DVD, Blu-ray): CSS - **Content Scramble System**, AACS - **Advanced Access Content System**

User authentication

… and much much more

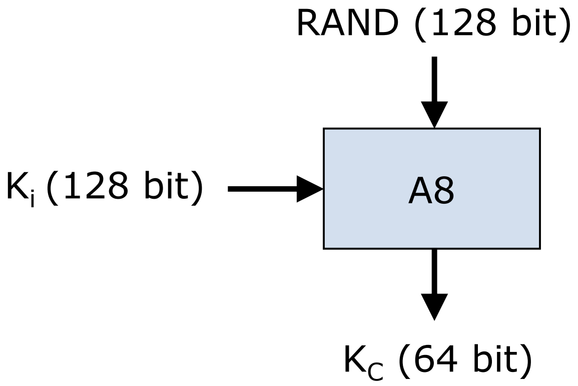
A3 – MS Authentication Algorithm

- Goal
  - Generation of SRES response to MSC’s random challenge RAND



A8 – Voice Privacy Key Generation Algorithm

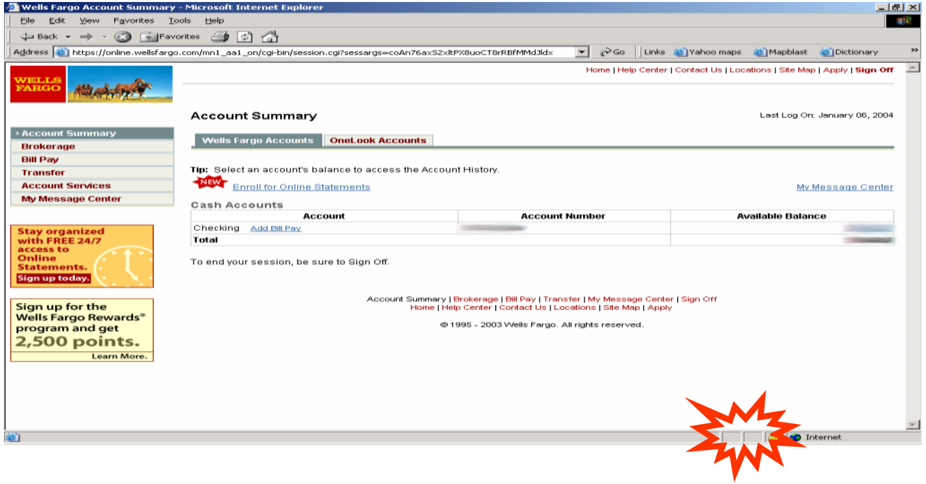
- Goal
  - Generation of session key K_s
    - A8 specification was never made public



A5 – Encryption Algorithm

- A5 is a stream cipher
  - Implemented very efficiently on hardware
  - Design was never made public
  - Leaked to Ross Anderson and Bruce Schneier
- Variants
  - A5/1 – the strong version
  - A5/2 – the weak version
  - A5/3
    - GSM Association Security Group and 3GPP design
    - Based on Kasumi algorithm used in 3G mobile systems

Secure communication


Wells Fargo Account Summary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Favorites
Address https://online.wellsfargo.com/mn1_aa1_on/cgi-bin/session.cgi?sessargs=coAn76axS2xltPX8uoCT8rRBfMMdJldx
Go Links Yahoo maps Mapblast Dictionary
WELLS FARGO
Home | Help Center | Contact Us | Locations | Site Map | Apply | Sign Off
› Account Summary
Brokerage
Bill Pay
Transfer
Account Services
My Message Center
Stay organized with FREE 24/7 access to Online Statements. Sign up today.
Sign up for the Wells Fargo Rewards® program and get 2,500 points. Learn More.
Wells Fargo Accounts
OneLook Accounts
NEW
Internet

Account Summary

Last Log On: January 06, 2004

Tip: Select an account's balance to access the Account History.

Enroll for Online Statements

My Message Center

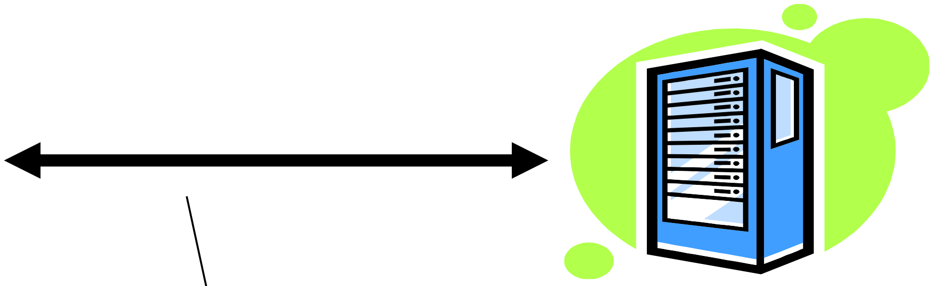
Cash Accounts

Account	Account Number	Available Balance
Checking Add Bill Pay	[redacted]	[redacted]
Total		[redacted]

To end your session, be sure to Sign Off.

Account Summary | Brokerage | Bill Pay | Transfer | My Message Center | Sign Off
Home | Help Center | Contact Us | Locations | Site Map | Apply

© 1995 - 2003 Wells Fargo. All rights reserved.



no eavesdropping
no tampering

Secure Sockets Layer / TLS

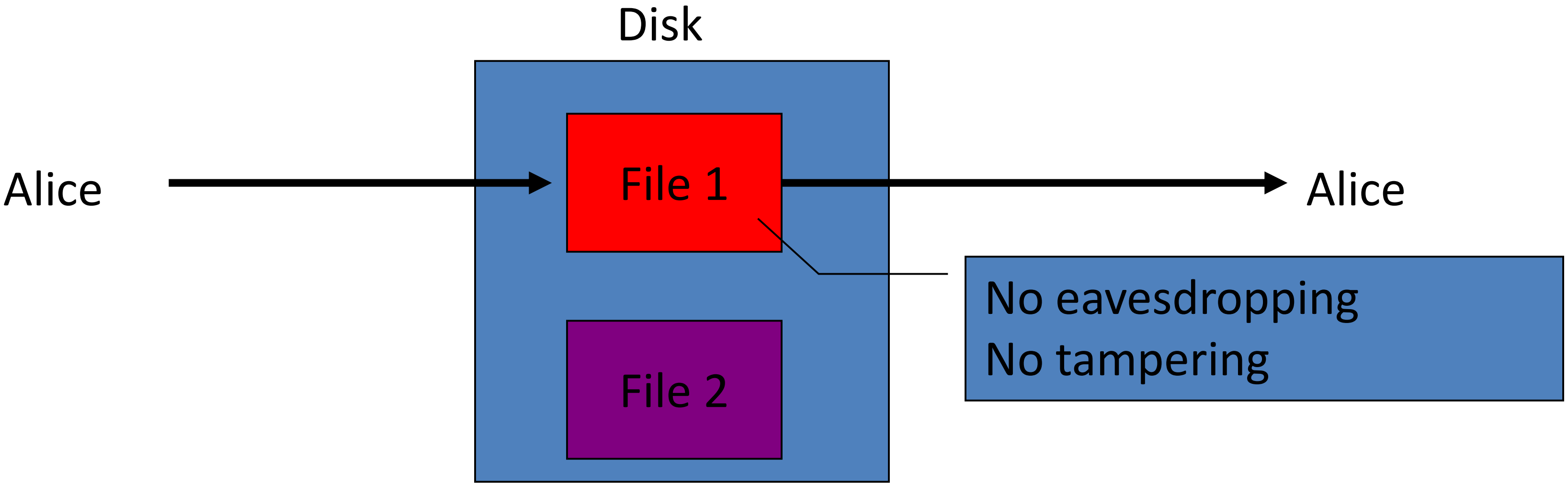
Two main parts

1. Handshake Protocol: **Establish shared secret key using public-key cryptography**

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

   Ensure confidentiality and integrity

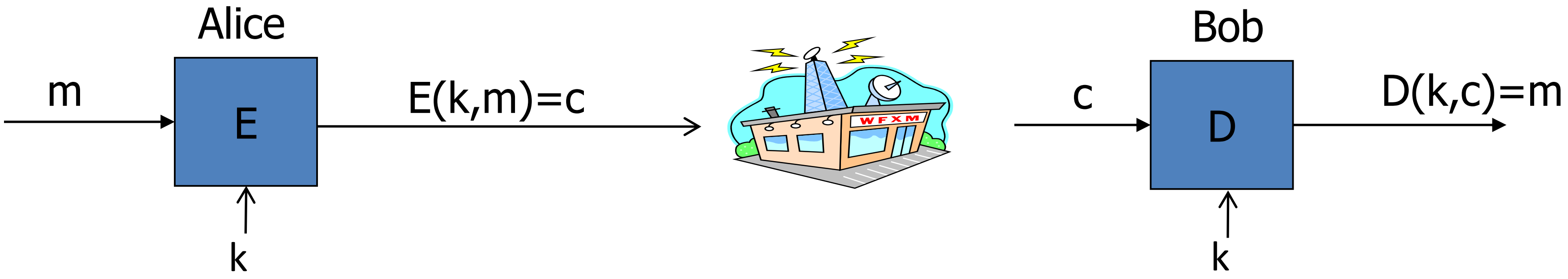
Protected files on disk



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

Use Cases

Single use key: (one time key)

- Key is only used to encrypt one message
  - encrypted email: new key generated for every email

Multi use key: (many time key)

- Key used to encrypt multiple messages
  - encrypted files: same key used to encrypt many files
- Need more machinery than for one-time key

Things to remember

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms

Cryptography is not:

- The solution to all security problems [s/w bug,social engg attacks]
- Reliable unless implemented and used properly
- Something you should try to invent yourself
    - many many examples of broken ad-hoc designs

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:

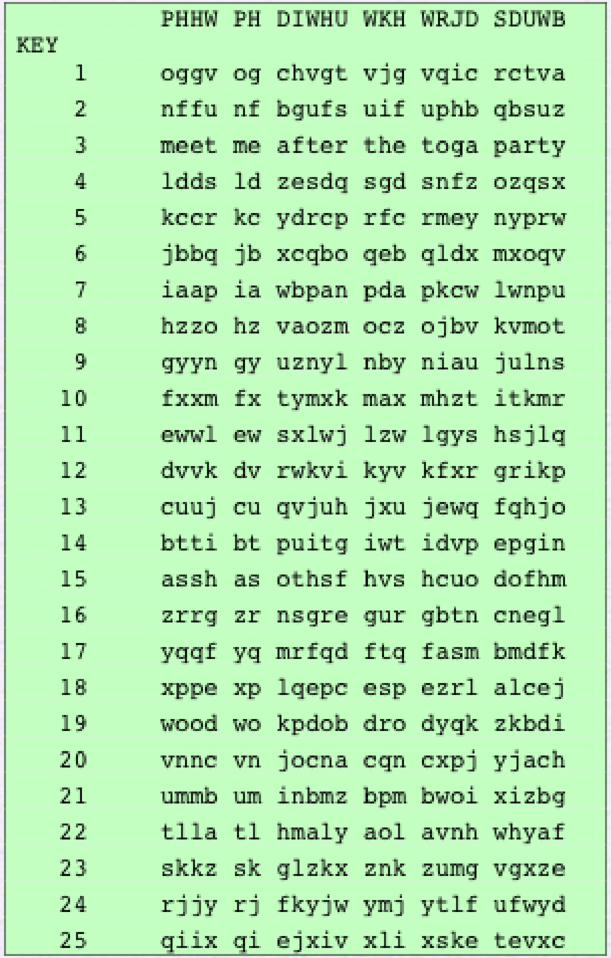
$$C = E(k, p) = (p + k) \mathit{mod}\ 26$$

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

$$p = D(k, C) = (C - k) \mathit{mod}\ 26$$

Brute-Force Cryptanalysis of Caesar Cipher

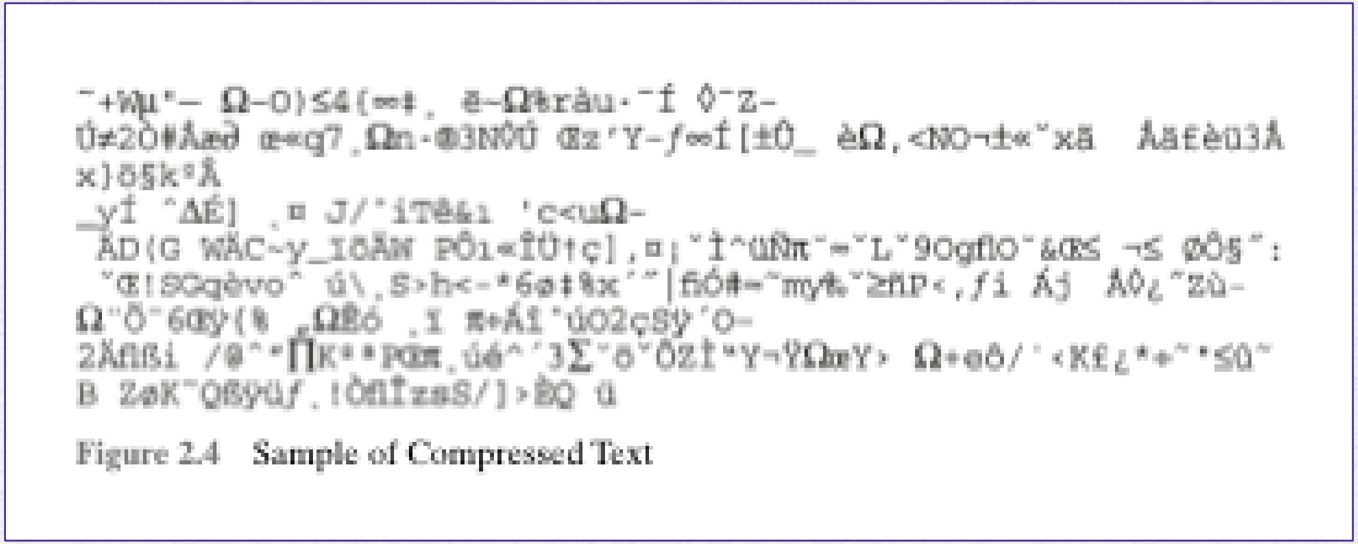
(This chart can be found on page 35 in the textbook)



	PHHW PH DIWHU WKH WRJD SDUWB
KEY	
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

Sample of Compressed Text



```
¯+Wµ˚— Ω–O}≤4{∞‡, ë–Ω‰ràu·¯ƒ ◊¯z–
Ú≠2Ò#Åæ∂ œ«q7,Ωn·®3NÒÚ Œz'Y–ƒ∞ƒ[±Ô_ èΩ,<NO¬±«˘xã  Åã£èü3Å
x}ö§k˚Å
_yƒ ˆ∆É] ,¤ J/ˆiTê&ı 'c<uΩ–
 ÅD(G WÄC~y_IõÅW PÔı«ÎÜ†ç],¤¡˘Ì^üÑπ˘=˘L˘9OgflO˘&Œ≤ ¬≤ ØÔ§˝:
 ˇŒ!SQqèvoˆ ú\,S›h<–*6ø‡‰x´˝|fiÓ#=˜my‰˘≥ñP‹,ƒi Áj ÅÔ¿˝zù–
Ω¨Õ¯6Œy{‰ „ΩÑó ,ı π+Áî˙úO2çSy´O–
2ÄñßI /®ˆ*∏K˚*PŒπ,úé^´3∑˘ö˘ÖZÌ*Y¬ŸΩæY› Ω+øô/˙‹K£¿*+˝*≤ü˝
B ZøK¯QßyÙƒ,!ÒñÎzæS/]›ÊQ ü
```

Figure 2.4 Sample of Compressed Text

Monoalphabetic Cipher

- Permutation
  - Of a finite set of elements *S* is an ordered sequence of all the elements of *S* , with each element appearing exactly once

- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4 x 10^{26} possible keys
  - This is 10 orders of magnitude greater than the key space for DES
  - Approach is referred to as a *monoalphabetic substitution cipher* because a single cipher alphabet is used per message

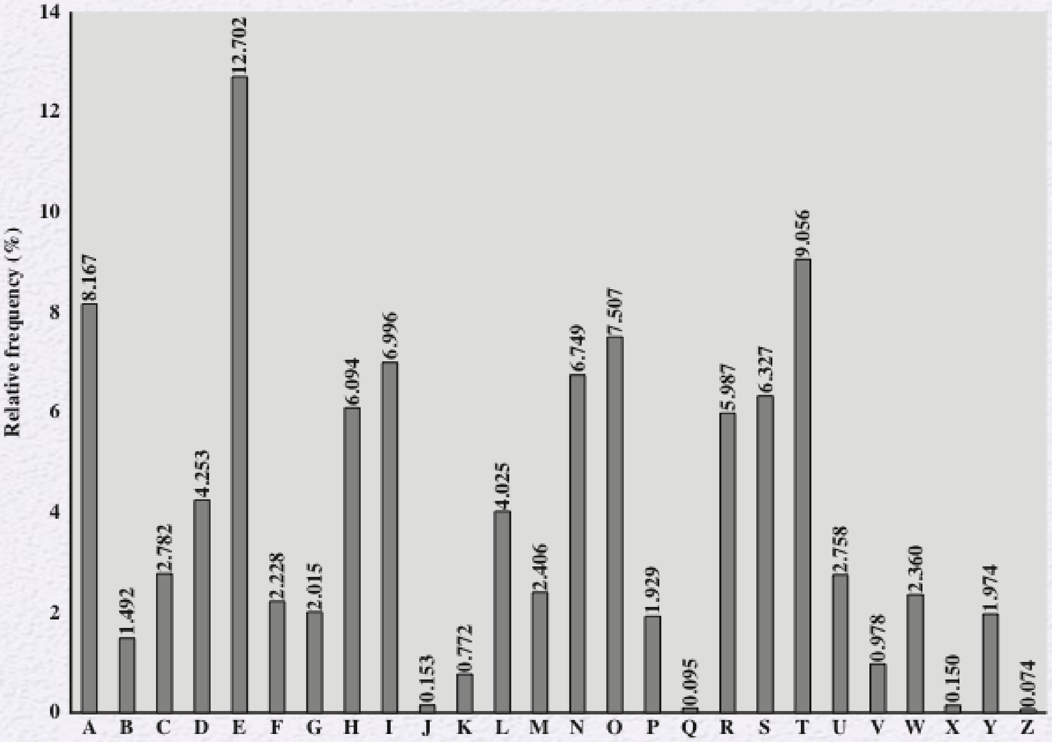
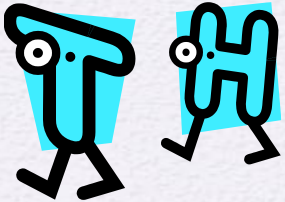


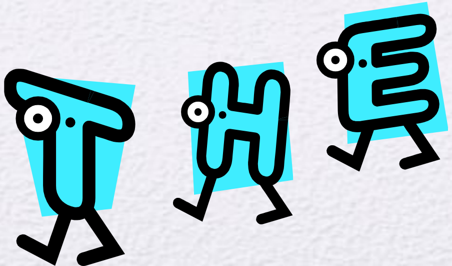
Figure 2.5 Relative Frequency of Letters in English Text

Monoalphabetic Ciphers

- Easy to break because they reflect the frequency data of the original alphabet
- Countermeasure is to provide multiple substitutes (homophones) for a single letter
- Digram
  - Two-letter combination
  - Most common is *th*



- Trigram
  - Three-letter combination
  - Most frequent is *the*



Playfair Cipher

- Best-known multiple-letter encryption cipher
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- Invented by British scientist Sir Charles Wheatstone in 1854
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

Playfair Key Matrix

- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order

- Using the keyword MONARCHY:

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

Rules

- 1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

- 2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.

- 3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.For example, mu is encrypted as CM

- 4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

- The Playfair cipher is a great advance over simple monoalphabetic ciphers.For one thing, whereas there are only 26 letters, there are 26 * 26 = 676 digrams, so that identification of individual digrams is more difficult. Furthermore, the relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult. For these reasons, the Playfair cipher was for a long time considered unbreakable.

- Despite this level of confidence in its security, the Playfair cipher is relatively

easy to break, because it still leaves much of the structure of

- It was used as the standard field system by the British Army in World War I and still enjoyed considerable use by the U.S. Army and other Allied forces during World War II.

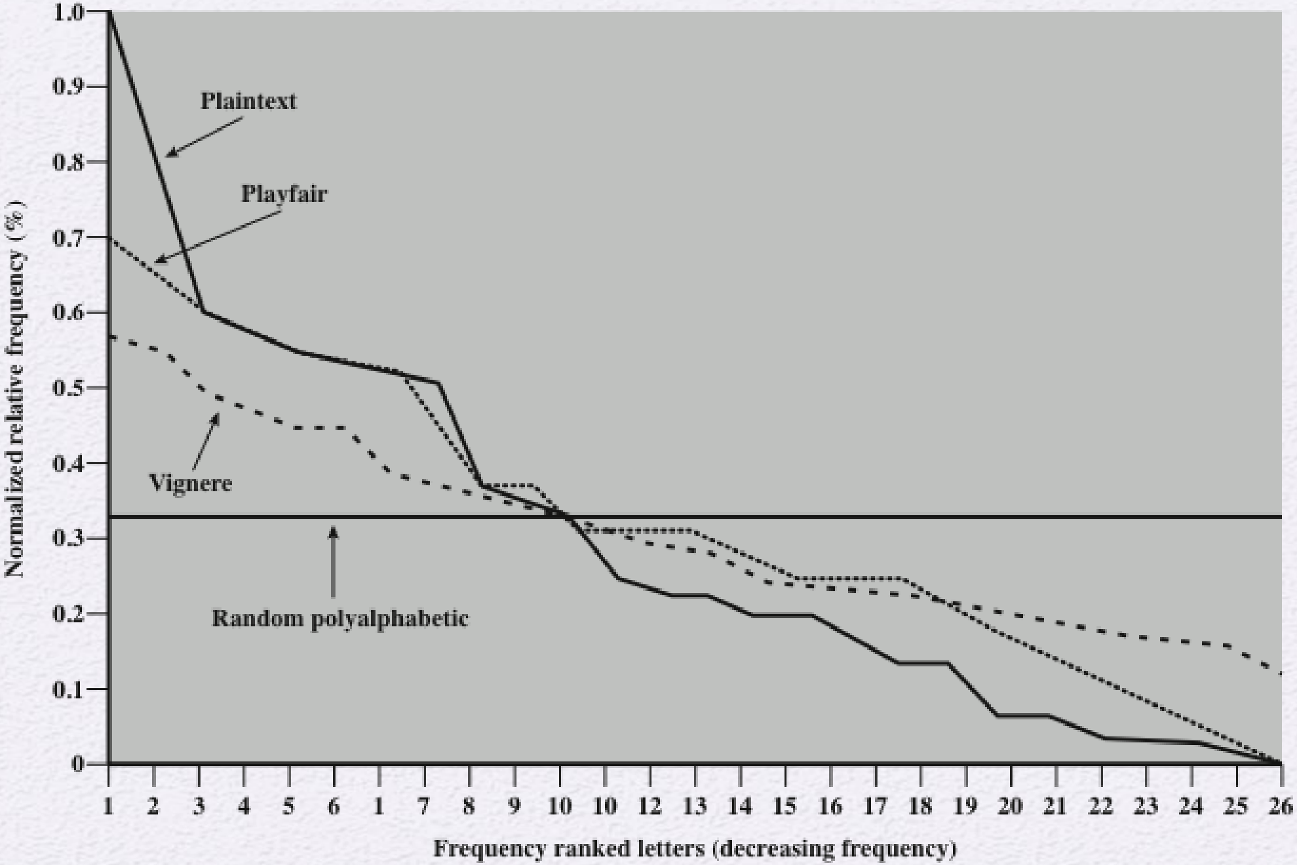


Figure 2.6 Relative Frequency of Occurrence of Letters

Cryptographic algorithms and protocols can be grouped into four main areas:

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

The field of network and Internet security consists of:

measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Computer Security

- The NIST *Computer Security Handbook* defines the term computer security as:

  "the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" (includes hardware, software, firmware, information/data, and telecommunications)

Computer Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

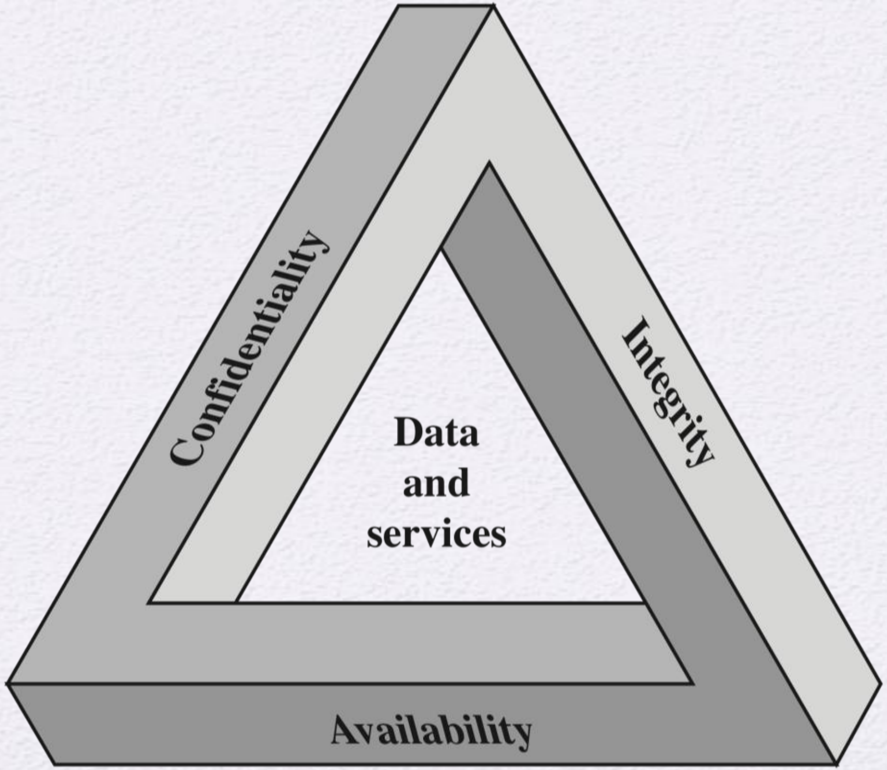
Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

CIA Triad


Confidentiality
Integrity
Data
and
services
Availability

Possible additional concepts:

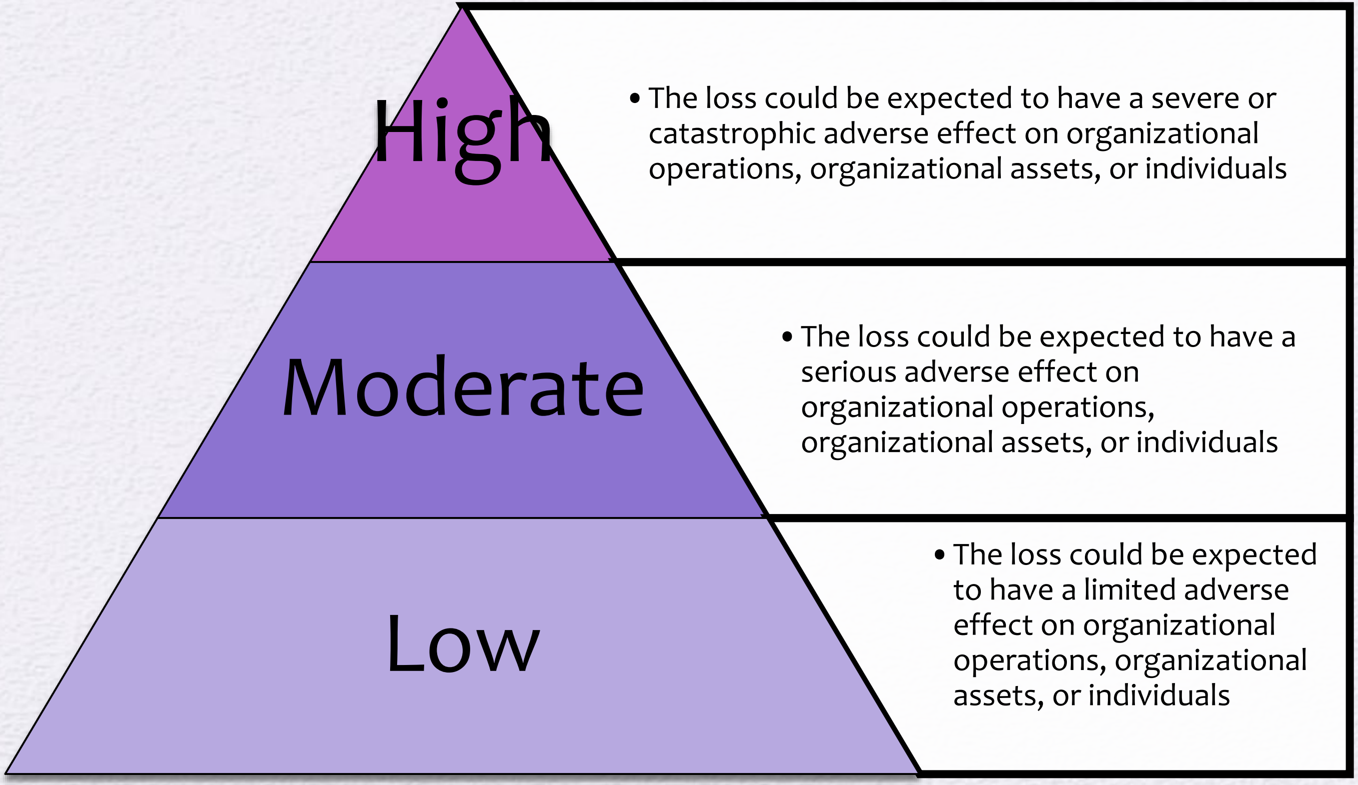
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Breach of Security
Levels of Impact



High

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Moderate

- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

Low

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought

- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

OSI Security Architecture

- Security attack
  - Any action that compromises the security of information owned by an organization
- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- Security service
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
  - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service