

(Network) Security

- All systems that have been designed, implemented and deployed, even the ones built by security experts, have security problems
- The evils of performance
 - Strict efficiency demands, even in areas where speed is not important
- The evils of features
 - Complexity is the worst enemy of security

Applied Cryptography

- Cryptography is a huge field
 - Computer security, higher algebra, economics, quantum physics, chip designs, quantum physics, etc.
- Applied cryptography
 - How to implement cryptography in real-world systems
- Role of cryptography
 - The lock
 - Small part of a much larger security system
- Weakest link property
 - A security system is only as strong as its weakest link
 - Weakest link depends on the situation

Threat Model

- Every system can be attacked; the whole point of security is to provide access to some people and not to others
 - You will always have to trust some people in some way, they can attack your system
- What's your threat model?
 - Very important to know what you are trying to protect against

Internet Threat Model (1/2)

- ``We assume that the actual end systems that the protocol is being executed on are secure ... We assume that the attacker has more or less complete control of the communications channel between any two machines.’’
- ``Protecting against attacks where one of the end systems is under the control of the attacker is extraordinarily difficult, if not impossible.’’

Internet Threat Model (2/2)

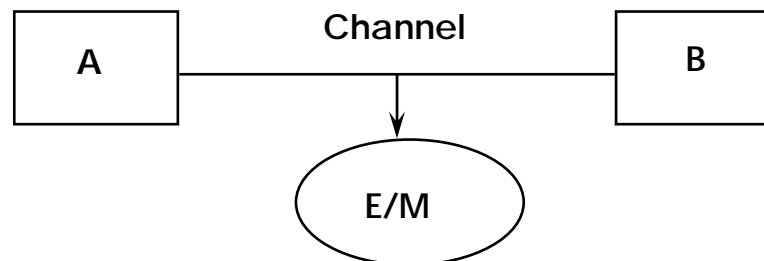
- We won't protect against the end system attack, because it is really difficult
- By the way, we'll ignore DOS because that's too difficult too
- But we'll cover the entire on-the-wire threats ... because we can!
- The threat model is about what we can protect; it is not a statement of what is needed for the application

Applied Cryptography Revisited

- Cryptography is not the solution
 - Protect the file or the key?
 - The areas that we understand well are small
 - Key management, key storage, and ...
 - Users
 - In the internet threat model, we have to protect the key

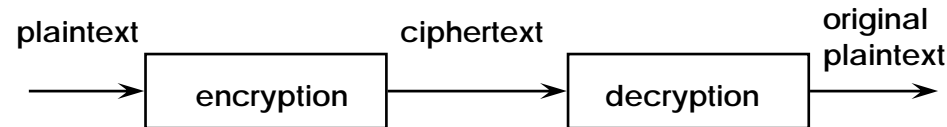
Real World

- The study of cryptosystems can be divided into:
 - Cryptography which concerns itself with the design of cryptosystems
 - Cryptanalysis which is the study of breaking of cryptosystems
- Data encryption:
 - Assures security of data on communication lines from attacks of two types
 - Passive: The attacker can capture and study the exchanged traffic
 - Active: Attacker is able to modify, inject, replay exchanged messages



Encryption

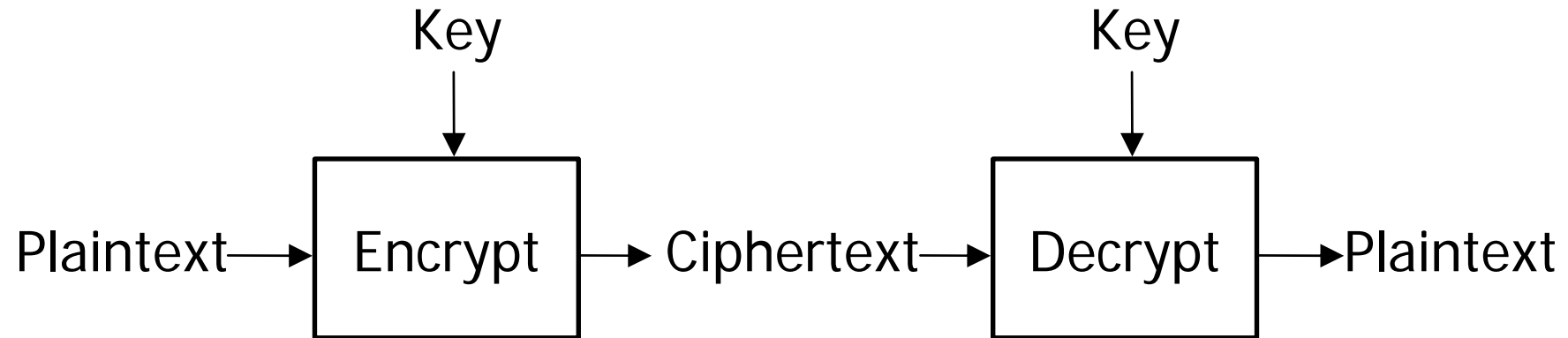
- The original data to be transferred is called *plaintext*
- The encrypted (protected) version is called *ciphertext*



- Plaintext is denoted P , whereas ciphertext is denoted C
 - Encryption function E operates on P to produce C
 - * $E(P) = C$
- In the reverse process
 - The decryption function D operates on C to produce P
 - * $D(C) = P$
- The following identity must also hold true for the cryptosystem to function correctly
 - * $D(E(P)) = P$

Encryption/Decryption Keys

- All modern encryption algorithms use a *key* denoted by K
- The key can take on many possible values
 - The range of possible values is called the *key space*



- The encryption and decryption functions now become
 - $E_k(P) = C$
 - $D_k(C) = P$

Kerckhoff's Principle

- The security of the encryption scheme must depend only on the secrecy of the key K , and not on the secrecy of the algorithms
- Algorithms:
 - Are hard to change
 - Is hard enough to keep a simple key secret
 - Should be published

Substitution Ciphers

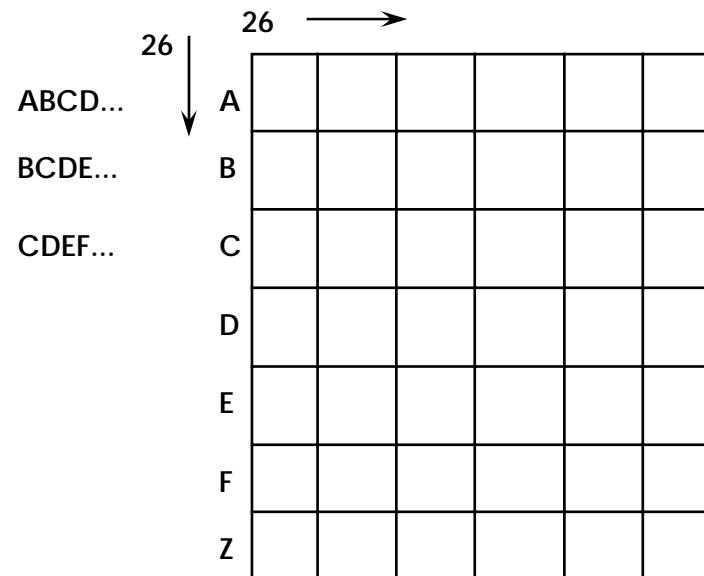
- In a substitution cipher
 - Each letter or a group of letters is replaced by another letter or group of letters to disguise it
- Caesar cipher
 - Mono-alphabetical substitution
 - In this system the alphabet is written out twice:

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

- To send a secret message
 - The letters of the message are taken one by one and the letters appearing below are written instead
- The message ``send spears'' would be enciphered as ``VHQQ VSHDUV''
- Attack
 - Use the properties of natural language
 - * Look for most commonly occurring characters
 - e, t, o, a, n, i
 - Look for domain specific words
 - * system, login, passwd, money

Polyalphabetical Ciphers

- Some protection from the above can be gained by using a number of different alphabets in rotation
 - Create a matrix of 26 different alphabets



- Now pick a key
 - E.g.: AFGHANISTANHELLOWORLD
- Use row A to encrypt first letter of plaintext, row F the second letter etc.

One Time Key (Pad)

- Choose a random number as a key
- The number should be longer than or equal to the message
- XOR the key with the message
 - Bitwise operation with two inputs where the output bit is 1 if exactly one of the two input bits is one
 - $(B \text{ XOR } A) \text{ XOR } A = B$
 - Results in an un-breakable code as all characters have equal probability
- The method is
 - Cumbersome to manage
 - Limits the message size
- Once the key is used more than once
 - All advantages are lost
 - Eve now has some details regarding the probability of the output bits, hence about the key

Transpositional Ciphers

- Substitution ciphers preserve the order of the text symbols but disguise them
- Transposition ciphers reorder the symbols
 - Do not disguise them
- The plaintext is written horizontally in rows
- Ciphertext is read out in columns
 - Starting with the column whose key is the lowest

<u>M</u>	<u>E</u>	<u>G</u>	<u>A</u>	<u>B</u>	<u>U</u>	<u>C</u>	<u>K</u>
<u>7</u>	<u>4</u>	<u>5</u>	<u>1</u>	<u>2</u>	<u>8</u>	<u>3</u>	<u>6</u>
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	i	o	n	
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d


Plaintext□

pleasetransferonemilliondollarsto
myswissbankaccountsixtwo[

Ciphertext□

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT□
ESILYNTWRNNTSOWDPAEDOBUCERIRICXB

Strength of Cryptosystems

- 
- The goal is to find the key
 - Remember the algorithm is publicly known
 - Ciphertext only
 - Attacker has access to encrypted data, but nothing else
 - Known plaintext
 - Attacker may know or guess all or part of the encrypted plaintext
 - Chosen plaintext
 - Attacker can choose plaintext to encrypt and may examine the resulting ciphertext
 - Chosen ciphertext (and plaintext)
 - Attacker can choose both plaintext and ciphertext
 - For every plaintext chosen, gets the corresponding ciphertext
 - For every ciphertext chosen, gets the corresponding plaintext