Introduction

The Cast of Characters

- Alice and Bob are the good guys

- Trudy is the bad guy

- Trudy is our generic “intruder”

Alice's Online Bank

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice and Bob concerns similar? How are they different?
- How does Trudy view the situation?

CIA

- Confidentiality, Integrity, and Availability
- AOB must prevent Trudy from learning Bob's account balance
- **Confidentiality:** prevent unauthorized reading of information

CIA

- Trudy must not be able to change Bob's account balance
- Bob must not be able to improperly change his own account balance
- **Integrity:** prevent unauthorized writing of information

CIA

- AOB's information must be available when needed
- Alice must be able to make transaction
  - If not, she'll take her business elsewhere
- **Availability:** Data is available in a timely manner when needed
- Availability is a "new" security concern
  - In response to denial of service (DoS)

Beyond CIA

- How does Bob's computer know that "Bob" is really Bob and not Trudy?
- Bob's password must be verified
    - This requires some clever **cryptography**
- What are security concerns of pwds?
- Are there alternatives to passwords?

Beyond CIA

- When Bob logs into AOB, how does AOB know that "Bob" is really Bob?
- As before, Bob's password is verified
- Unlike standalone computer case, network security issues arise
- What are network security concerns?
- **Protocols** are critically important
- Crypto also important in protocols

Beyond CIA

- Once Bob is *authenticated* by AOB, then AOB must restrict actions of Bob
  - Bob can't view Charlie's account info
  - Bob can't install new software, etc.
- Enforcing these restrictions is known as *authorization*
- **Access control** includes both authentication and authorization

Beyond CIA

- Cryptography, protocols, and access control are implemented in **software**
- What are security issues of software?
  - Most software is complex and buggy
  - Software flaws lead to security flaws
  - How to reduce flaws in software development?

Beyond CIA

- Some software is intentionally evil
  - Malware: computer viruses, worms, etc.
- What can Alice and Bob do to protect themselves from malware?
- What can Trudy do to make malware more “effective”?

Beyond CIA

- Operating systems enforce security
  - For example, authorization
- OS: large and complex software
  - Win XP has 40,000,000 lines of code!
  - Subject to bugs and flaws like any other software
  - Many security issues specific to OSs
  - Can you trust an OS?

Our Book

- The text consists of four major parts
  - Cryptography
  - Access control
  - Protocols
  - Software

Cryptography

- "Secret codes"
- The book covers
  - Classic cryptography
  - Symmetric ciphers
  - Public key cryptography
  - Hash functions
  - Advanced cryptanalysis

Access Control

- Authentication
  - Passwords
  - Biometrics and other
- Authorization
  - Access Control Lists and Capabilities
  - Multilevel security (MLS), security modeling, covert channel, inference control
  - Firewalls and Intrusion Detection Systems

Protocols

- Simple authentication protocols
  - "Butterfly effect" — small change can have drastic effect on security
  - Cryptography used in protocols
- Real-world security protocols
  - SSL, IPSec, Kerberos
  - GSM security

Software

- Software security-critical flaws
  - Buffer overflow
  - Other common flaws
- Malware
  - Specific viruses and worms
  - Prevention and detection
  - The future of malware

Software

- Software reverse engineering (SRE)
  - How hackers "dissect" software
- Digital rights management (DRM)
  - Shows difficulty of security in software
  - Also raises OS security issues
- Limits of testing
  - Open source vs closed source

Software

- Operating systems
  - Basic OS security issues
  - “Trusted” OS requirements
  - NGSCB: Microsoft’s trusted OS for PC
- Software is a big security topic
  - Lots of material to cover
  - Lots of security problems to consider

Think Like Trudy

- In the past, no respectable sources talked about "hacking" in detail
- It was argued that such info would help hackers
- Very recently, this has changed
  - Books on network hacking, how to write evil software, how to hack software, etc.

Think Like Trudy

- Good guys must think like bad guys!
- A police detective
  - Must study and understand criminals
- In information security
  - We want to understand Trudy's motives
  - We must know Trudy's methods
  - We'll often pretend to be Trudy

Think Like Trudy

- Is all of this security information a good idea?
- "It's about time somebody wrote a book to teach the good guys what the bad guys already know." — Bruce Schneier

Think Like Trudy

- We must try to think like Trudy
- We must study Trudy's methods
- We can admire Trudy's cleverness
- Often, we can't help but laugh at Alice and Bob's stupidity
- But, we **cannot** act like Trudy

In This Course…

- Always think like the bad guy
- Always look for weaknesses
- Strive to find a weak link
- It's OK to break the rules
- Think like Trudy!
- But don't do anything illegal…

Crypto Basics

Crypto

- ❑ **Cryptology** — The art and science of making and breaking "secret codes"
- ❑ **Cryptography** — making "secret codes"
- ❑ **Cryptanalysis** — breaking "secret codes"
- ❑ **Crypto** — all of the above (and more)

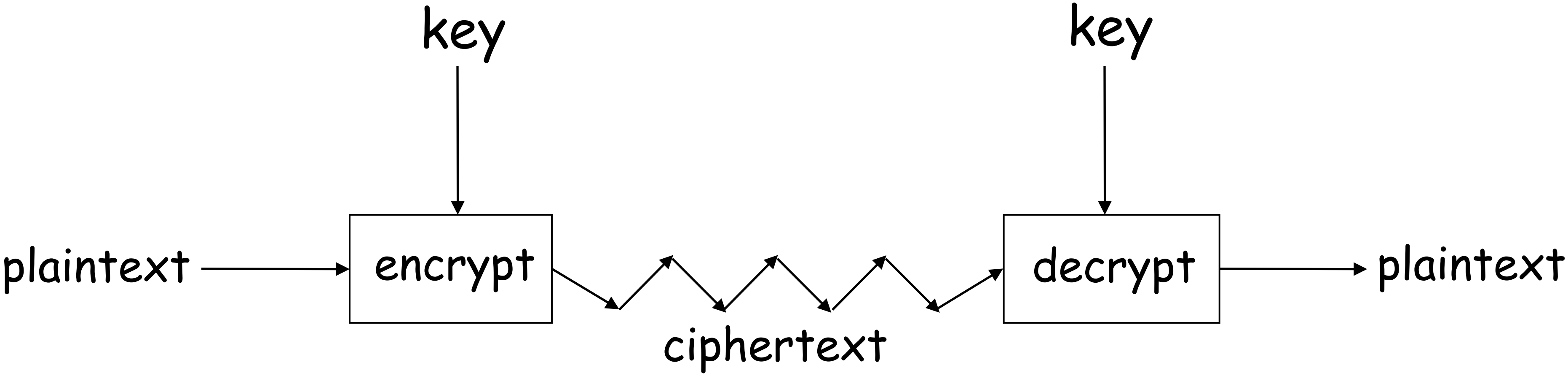
How to Speak Crypto

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt (sign)

Crypto

- Basic assumption
  - The system is completely known to the attacker
  - Only the key is secret
- Also known as **Kerckhoffs Principle**
  - Crypto algorithms are not secret
- Why do we make this assumption?
  - Experience has shown that secret algorithms are weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

Crypto as Black Box



A generic use of crypto

Simple Substitution

- Plaintext: fourscoreandsevenyearsago
- Key:

Plaintext	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
Ciphertext	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

Simple Substitution

- Plaintext: fourscoreandsevenyearsago
- Key:

Plaintext	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
Ciphertext	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

- Ciphertext:

  IRXUVFRUHDAGVHYHABHDUVDIR
- Shift by 3 is "Caesar's cipher"

Ceasar's Cipher Decryption

- Suppose we know a Ceasar's cipher is being used
- Ciphertext: VSRQJHEREVTXDUHSDQWU

Plaintext	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
Ciphertext	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

Ceasar's Cipher Decryption

- Suppose we know a Ceasar's cipher is being used
- Ciphertext:
  VSRQJHEREVTXDUHSDQWU

Plaintext	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
Ciphertext	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

- Plaintext: spongebobsquarepants

Not-so-Simple Substitution

- Shift by n for some n ∈ {0,1,2,…,25}
- Then key is n
- Example: key = 7

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

Cryptanalysis I: Try Them All

- A simple substitution (shift by n) is used
- But the key is unknown
- Given ciphertext: CSYEVIXIVQMREXIH
- How to find the key?
- Only 26 possible keys — try them all!
- **Exhaustive key search**
- Solution: key = 4

Even-less-Simple Substitution

- Key is some permutation of letters
- Need not be a shift
- For example

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

- How many possible keys do we have now?

Even-less-Simple Substitution

- Key is some permutation of letters
- Need not be a shift
- For example

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

- 26! > 2^{88} possible keys!