CISC 7320X – COMPUTER SECURITY

Cryptography

Topics for today

- Cryptography:
  - Problems encryption is designed to solve
  - Encryption tools categories, strengths, weaknesses
    - applications of each
  - Certificates and certificate authorities

CRYPTOGRAPHY

https://www.tripwire.com/state-of-security/security-data-protection/cryptography/ordinary-people-need-cryptography/

Communication Security

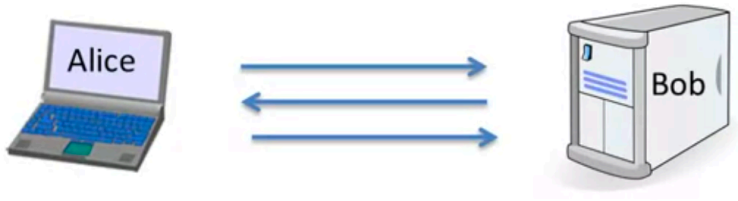
- Protects messages on route from sender to recipient
- An attacker may attempt to:
  - Intercept the message
  - Modify the message
  - Fabricate an authentic-looking alternate message
  - Block the message
- Encryption used to ensure secrecy of message
- Authentication used to ensure integrity

Encryption

- Taking a ***Plaintext*** message
- Applying a ***Cipher*** operation to it
- Results in an unreadable garbled ***Ciphertext*** message

Communication Security

- Two parties trying to communicate
- An eavesdropper tries to intercept message



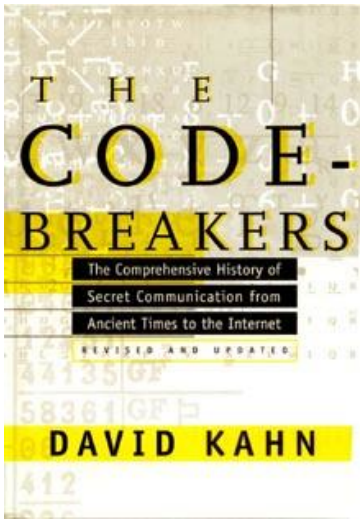
HISTORY

History

- Codes and ciphers usage began as early as 1900 BCE
- Classic cryptography used pen and paper
  - Or mechanical aids
- Mathematical models started developing in the 19th century
  - World war I and II

History of Cryptography

David Kahn, “The code breakers” (1996)



Caesar Cipher: c = m + 3

A B C D E F G H I J

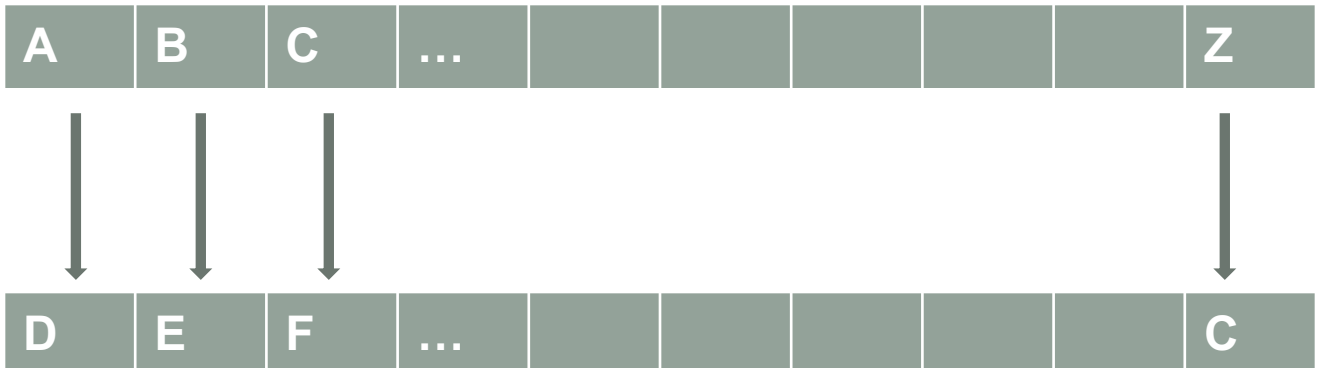
K L M N O P Q R

S T U V W X Y Z

Julius Caesar
100 BC- 44 BC

Caesar cipher

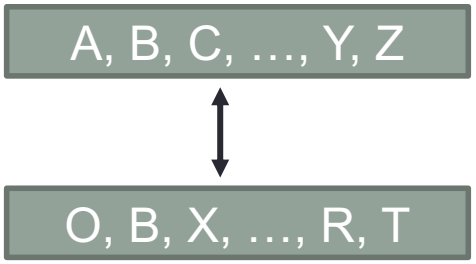
- Shift by some number of characters
  - Size of shift is a key (example = 3)



- Example: ‘cat’ -> ?
  - ‘cat’ -> ‘fdw’

Substitution Ciphers

- More generally, each letter is uniquely replaced by another
- How many different substitution ciphers are there?

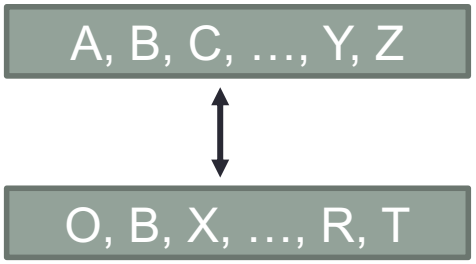


An arbitrary permutation of A,…, Z

Public domain image from http://en.wikipedia.org/wiki/File:ROT13.png

Substitution Ciphers

- More generally, each letter is uniquely replaced by another
- How many different substitution ciphers are there?



An arbitrary permutation of A,…, Z

- There are $26! \approx 4 \times 10^{26}$ such ciphers

Public domain image from http://en.wikipedia.org/wiki/File:ROT13.png

Substitution ciphers

- Key = substitution matrix
  - Example:

A	B	C	…						Z
R	M	G							A

  - Encrypt ‘ABC’:
    - ‘ABC’ -> ‘RMG’
- How many keys are possible?
  - Size of key space = 26!
    - That’s a huge number to search through, even for a computer

Letter encoding

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2: Encoding English capital letters using integers from $\mathbb{Z}_{26}$.

http://mvngu.wordpress.com/2008/08/20/the-shift-cipher-using-parigp/

Why are they vulnerable?

- Frequency Analysis:
  - Letters in a natural language, like English, are not uniformly distributed
  - Knowledge of letter frequencies, can be used in cryptologic attacks against substitution ciphers
    - including pairs and triples

Frequency Analysis

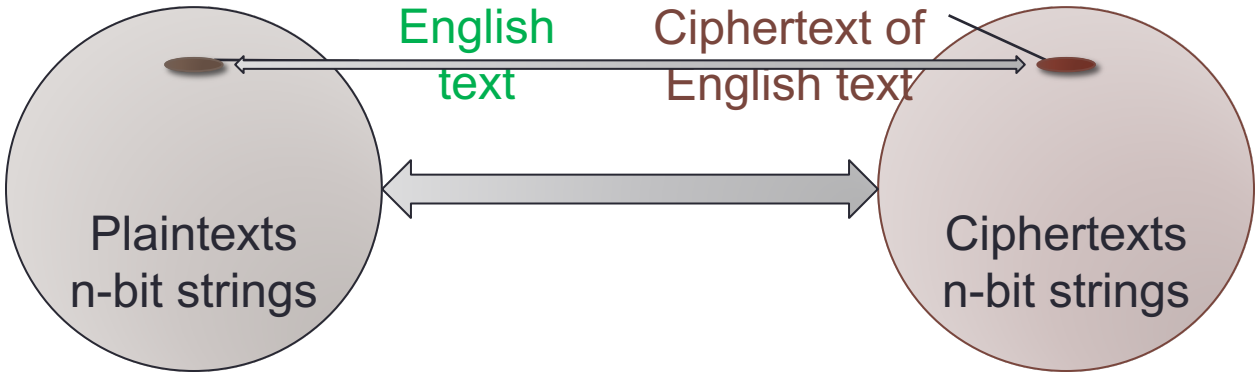
- Single letter frequency analysis:

a:	8.05%	b:	1.67%	c:	2.23%	d:	5.10%
e:	12.22%	f:	2.14%	g:	2.30%	h:	6.62%
i:	6.28%	j:	0.19%	k:	0.95%	l:	4.08%
m:	2.33%	n:	6.95%	o:	7.63%	p:	1.66%
q:	0.06%	r:	5.29%	s:	6.02%	t:	9.67%
u:	2.92%	v:	0.82%	w:	2.60%	x:	0.11%
y:	2.04%	z:	0.06%				

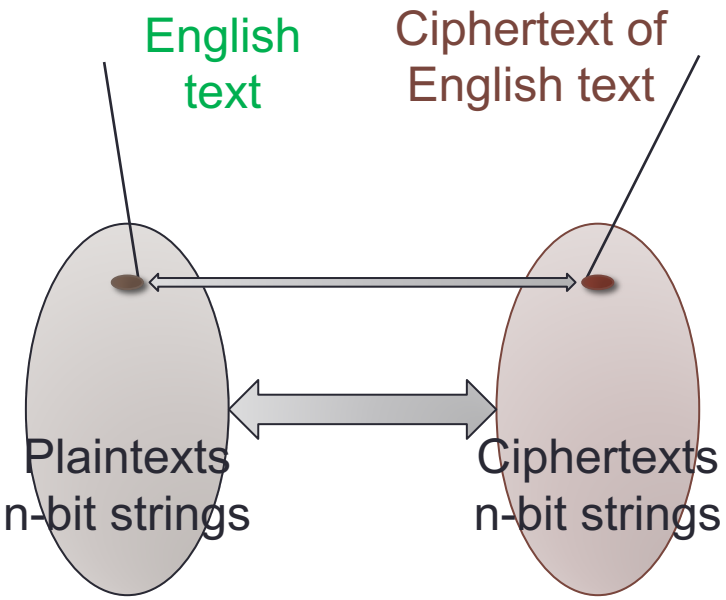
8.1: Letter frequencies in the book *The Adventures of Tom Sawyer*, by Twain.

Encrypting English Text

- English text typically represented with 8-bit ASCII encoding
- A message with t characters corresponds to an n-bit array, with $n = 8t$
- Redundancy due to repeated words and patterns
  - E.g., “th”, “ing”
- English plaintexts are a very small subset of all n-bit arrays



Encrypting English Text



Entropy of Natural Language

- How much information can an alphabet with 8 characters carry?
  - 3 bits of information
  - $2^3 = 8$
- For the English language, each character can convey log (26) = 4.7 bits of information

Entropy of Natural Language

- However, meaningful English text is only ~1.25 bits per char
- Therefore, plaintext redundancy = 4.7 – 1.25 = 3.45
- For example, if a word has 8 characters, what is the effective dictionary size?
  - How many words on average will we have?
  - $2^{8*1.25} = 2^{10} = 1024$

Entropy of English Language

- How do you statistically calculate the entropy of the next letter when the previous $N - 1$ letters are known?
  - In a word
- As N increases, the entropy approaches the entropy of English

	F_0	F_1	F_2	F_3
26 letter	4.70	4.14	3.56	3.3

http://people.seas.harvard.edu/~jones/cscie129/papers/stanford_info_paper/entropy_of_english_9.htm

Entropy of English Language

- Do we include the space?
  - The 27-letter sequences include the space as a letter
  - Onecanalmostalwaysfillinthespacesfromasequenceofwordswithnospaces
  - Therefore, spaces are basically redundant
    - will cause lower calculated entropies when taken into account

Entropy of English Language

- Do we include the space?
  - Entropy of each letter in a string in English:

	F_0	F_1	F_2	F_3
26 letter	4.70	4.14	3.56	3.3
27 letter	4.76	4.03	3.32	3.1

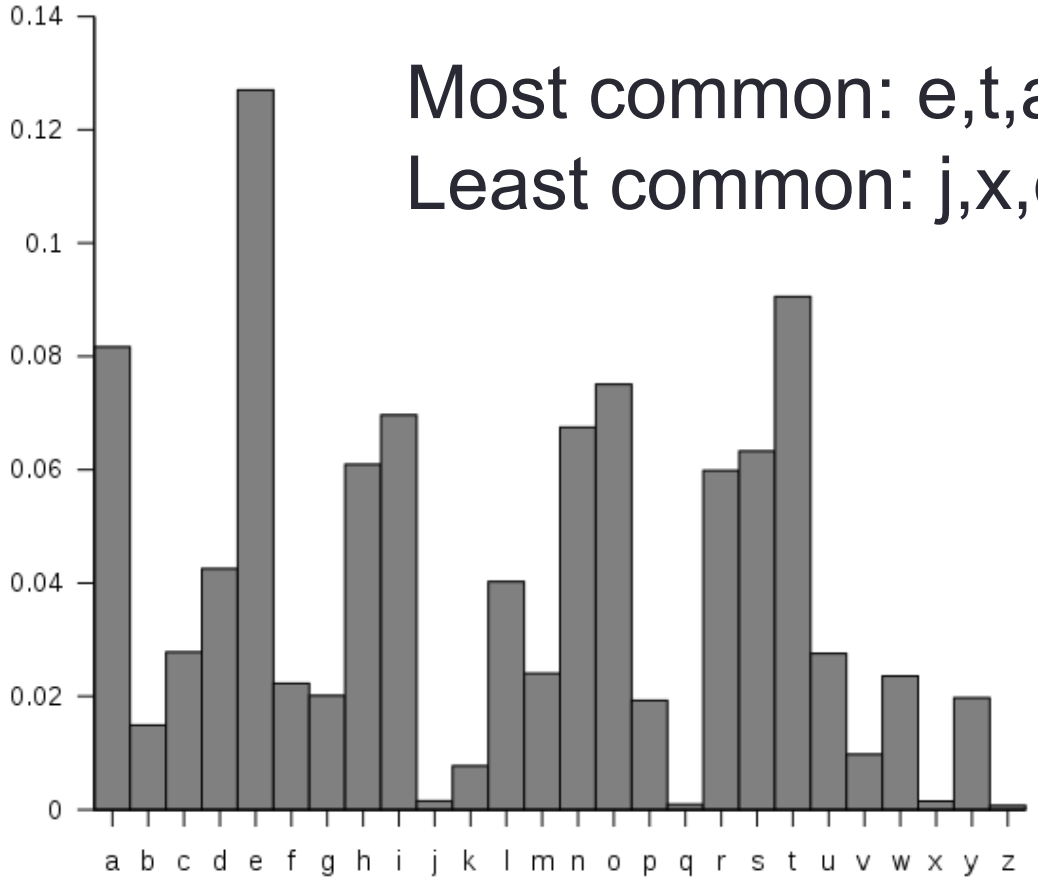
    - Spaces are basically redundant
      - will cause lower calculated entropies when taken into account
    - Only in the F_0 case, where no statistics are taken into account, is the entropy higher when the space is added
      - This simply adds another possible symbol, which means more uncertainty

http://people.seas.harvard.edu/~jones/cscie129/papers/stanford_info_paper/entropy_of_english_9.htm

Attacking Substitution Ciphers

Trick 1: *Word Frequency*

Trick 2: *Letter Frequency*



Most common: e,t,a,o,i,n

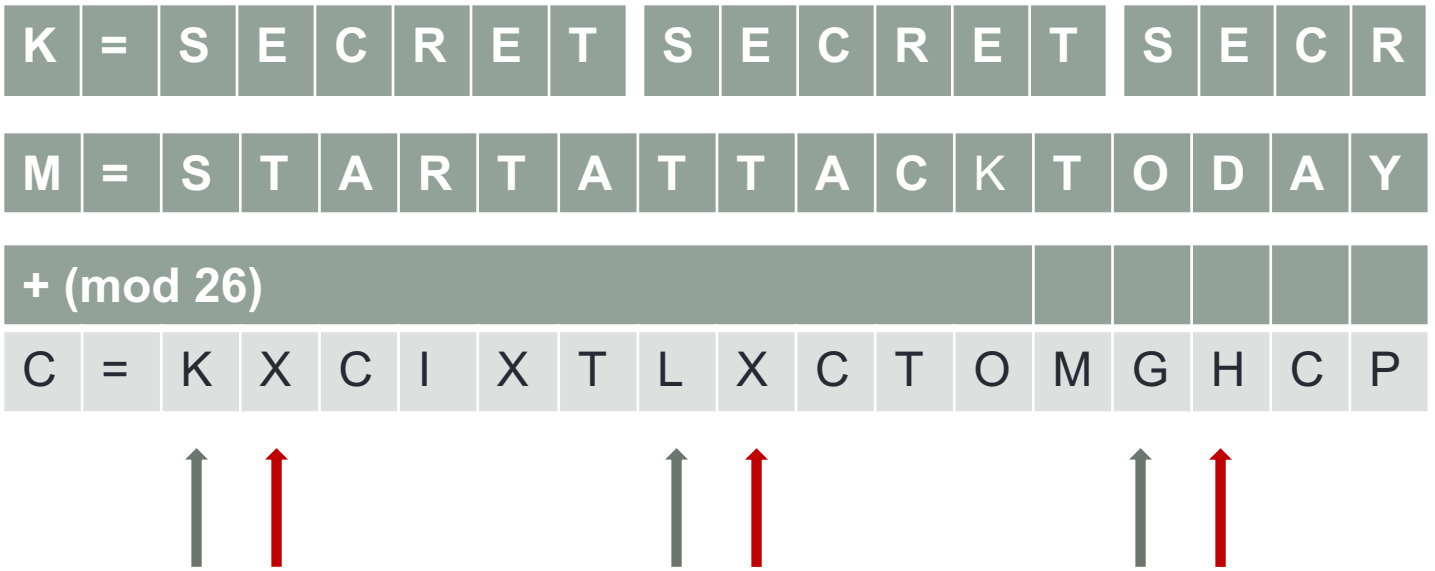
Least common: j,x,q,z

image source: wikipedia

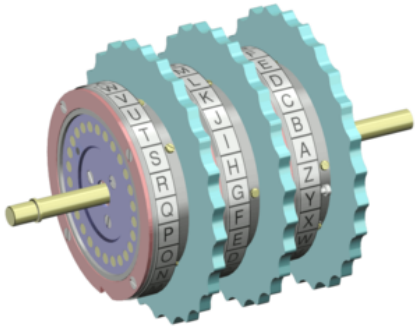
Jvl mlwclk yr jvl owmwez twp yusl w zyduo pjdcluj mqil zydkplmr. Hdj jvlz tykilc vwkc jy mlwku jvl wkj yr vwsiquo, tvqsv vlmflc mlwc jvlg jy oklwjulpp. Zyd vwnl jvl fyjlujqwm jy cy jvl pwgl. Zydk plsklj fwpptykc qp: JYWPJ

Vigenere Cipher (Rome, 16th' century)

- A series of different Caesar ciphers
  - Described by Giovan Battista Bellaso
    - Named for Blaise de Vigenère
  - Example:

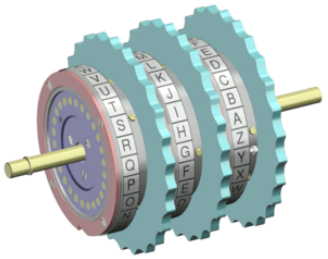


Mechanical Aids



- Rotor machine is an electro-mechanical stream cipher device used for encrypting and decrypting secret messages
  - Used in the 1920s–1970s
  - E.g., in the ***Enigma system***

Rotor machine



- Machine has rotating disks with an array of electrical contacts on either side
- Implements a fixed substitution of letters, replacing them in some complex fashion
- After encrypting each letter, the rotors advance positions, changing the substitution
- produces a complex substitution cipher, which changes with every keypress

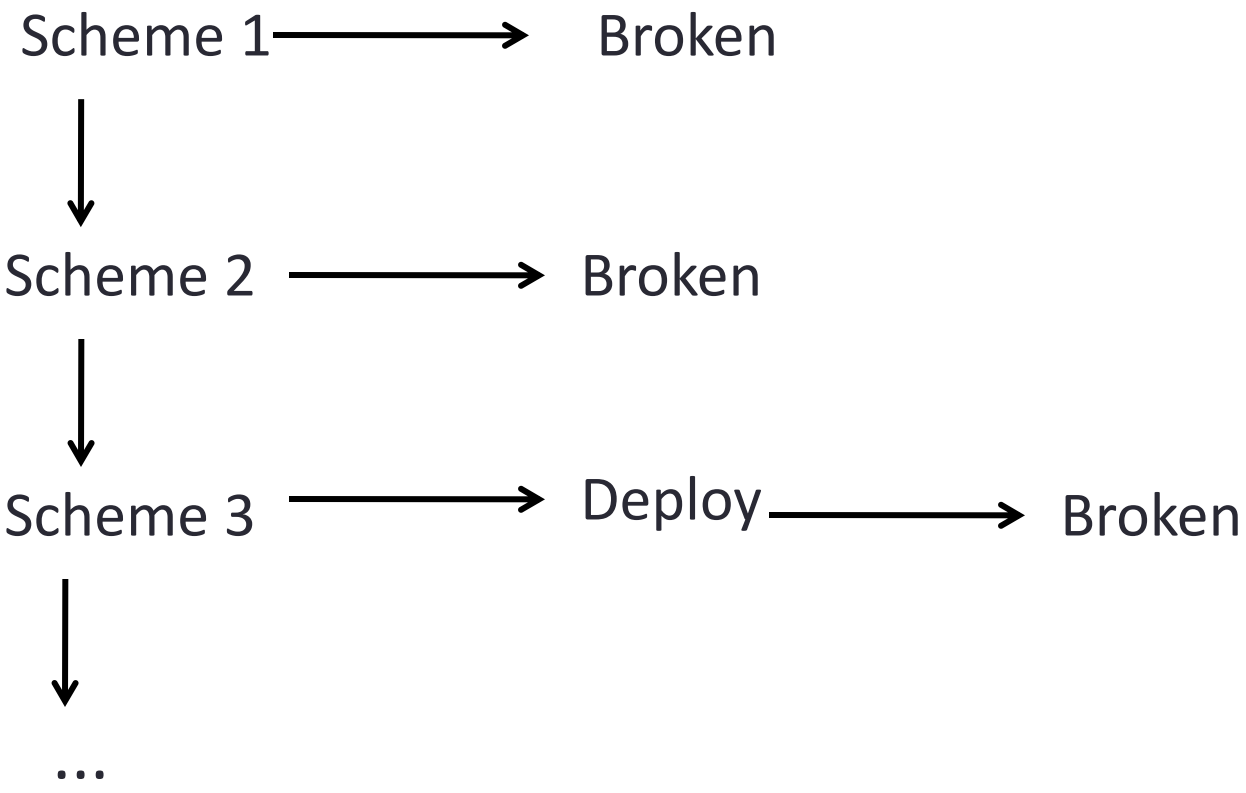
https://en.wikipedia.org/wiki/Rotor_machine

History

- During world war II, mathematical and statistical methods started being developed
- Successfully used to break into the German Enigma machine:
  - Messages were deciphered by the Allies
  - producing intelligence code-named Ultra

MODERN CRYPTOGRAPHY

Classical Approach: Iterated Design

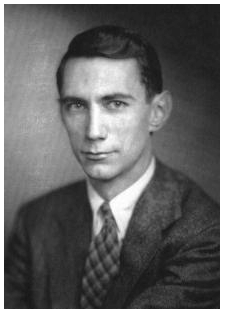


No way to say anything is secure
(and you may not know when broken)

Iterated design was only one we knew until 1945

Claude Shannon: 1916 - 2001

Claude Shannon



- Formally defined:
  - *security goals*
  - *adversarial models*
  - *security of system with regard to goals*
- Beyond iterated design: proof!

Encryption Terminology

- Sender
- Recipient/Receiver
- Transmission medium
- Interceptor/intruder/Attacker/Adversary
- Encrypt, encode, or encipher
  - Process that hides the meaning of the message
- Decrypt, decode, or decipher
  - Reveal the original message

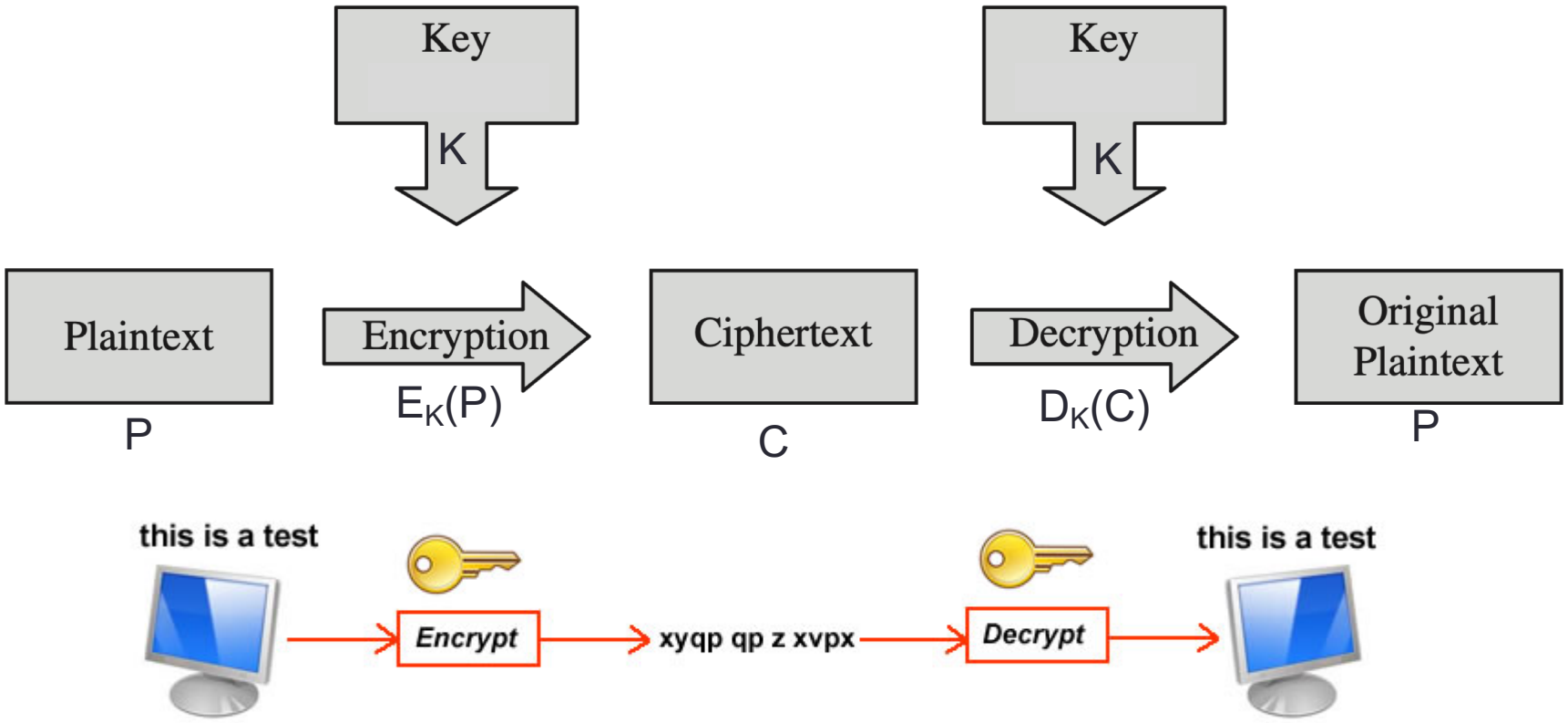
Encryption Terminology

- Cryptosystem
  - A system for encryption and decryption
- Plaintext
  - Original message
- Ciphertext
  - Encrypted message

Encryption Basics

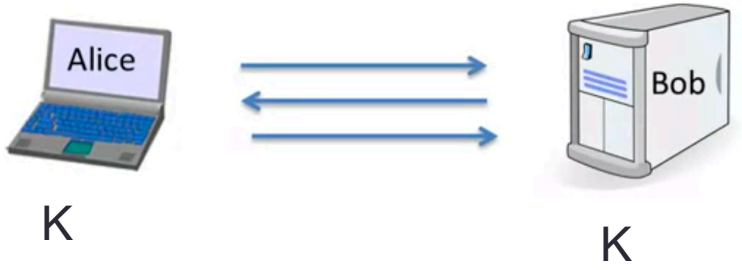
- Sender and Recipient often share a secret key
  - Known to them, but not anyone else
- An encryption process, used by sender
  - Takes plaintext and the key
  - Produces the encrypted ciphertext
- A decryption process, used by recipient
  - Takes ciphertext and the key
  - Recovers the original plaintext message

Encryption Basics

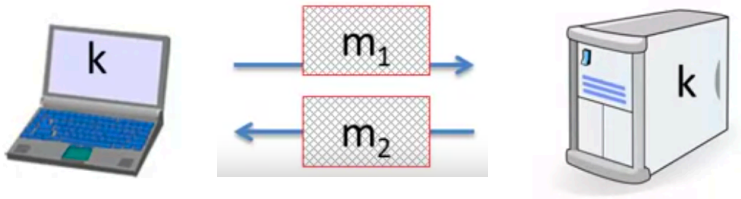


What is Cryptography?

- Two main functions:
  - Secret key establishment:
    - Both parties need to agree on a secret key



  - Secure communication:`
    - Use key to encrypt message
      - Provide confidentiality and integrrity

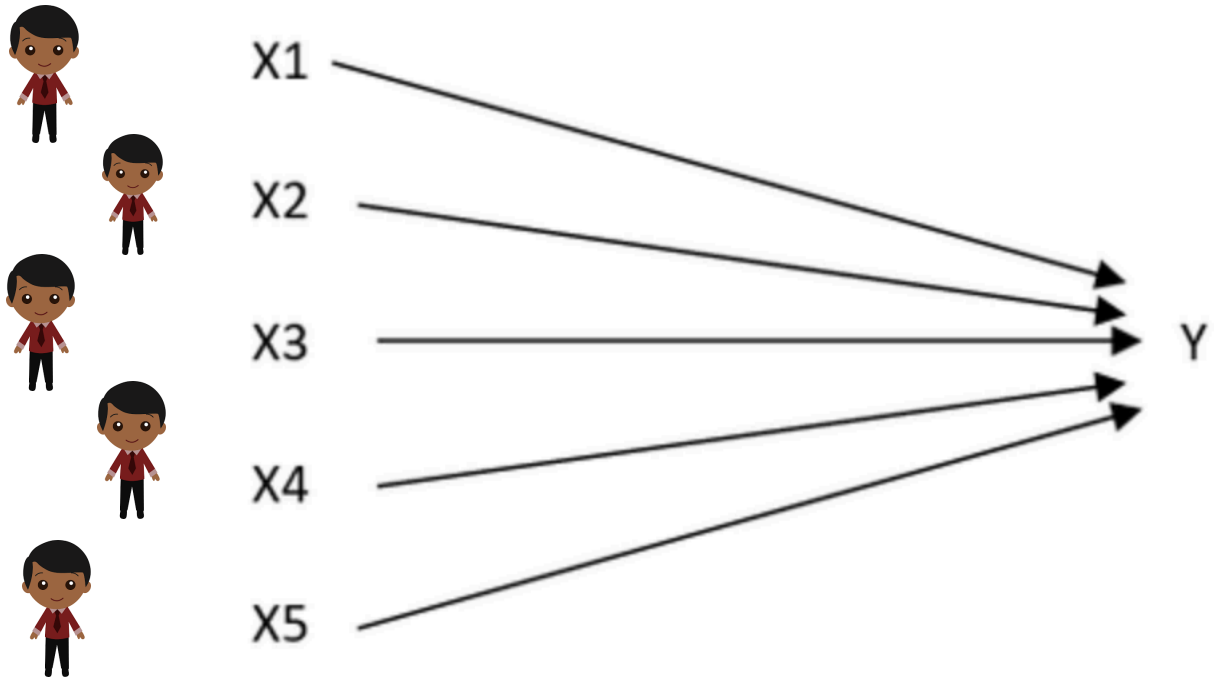


What is Cryptography?

- Digital Signatures
  - In the analog world, I can use the same signature to sign multiple documents
    - Not possible in the digital world
  - The signature has to be a function of the content being signed
    - Copying the signature from one document to the other will not work

What is Cryptography?

- Secure multi-party computation
  - Can be used to compute election, auction results



What is Cryptography?

- Secure multi-party computation (cont.)
  - Goal: Compute f(x1, x2, x3, x4, x5)
    - Can be done with a trusted party
      - i.e., ebay, election mechanism, etc.
  - Theorem:
    - Anything that can be done with a trusted authority, can also be done without
      - Through an algorithm
        - May take very long time, depending on the function calculated

What is Cryptography?

- Zero-Knowledge (proof of knowledge)
  - One party proves to the other that he knows something
    - Without sharing this data

What is Cryptography

- For each concept in cryptography:
  - Threat model has to be specified precisely
  - Solution is proposed
  - Breaking the solution will be hard
    - Too long to compute

Encryption Basics

- A cryptosystem involves a set of rules for how to encrypt a plaintext and decrypt the ciphertext
  - Rules == algorithms
- The resulting ciphertext depends on:
  - The algorithm (typically public and known to all)
  - The original message
  - The key value

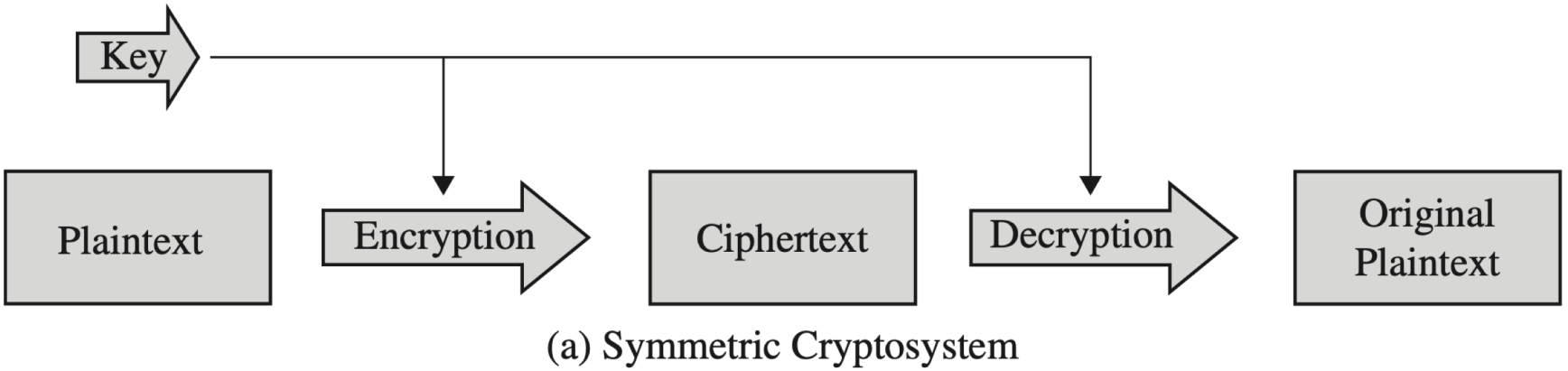
Symmetric Encryption

- Symmetric encryption uses the same key, K, both to encrypt a message and later to decrypt it
  - Also called single-key or secret key encryption
  - Uses a pair of efficient algorithms (E,D)
    - D and E are mirror-image processes
    - E is often randomized
    - D is always deterministic

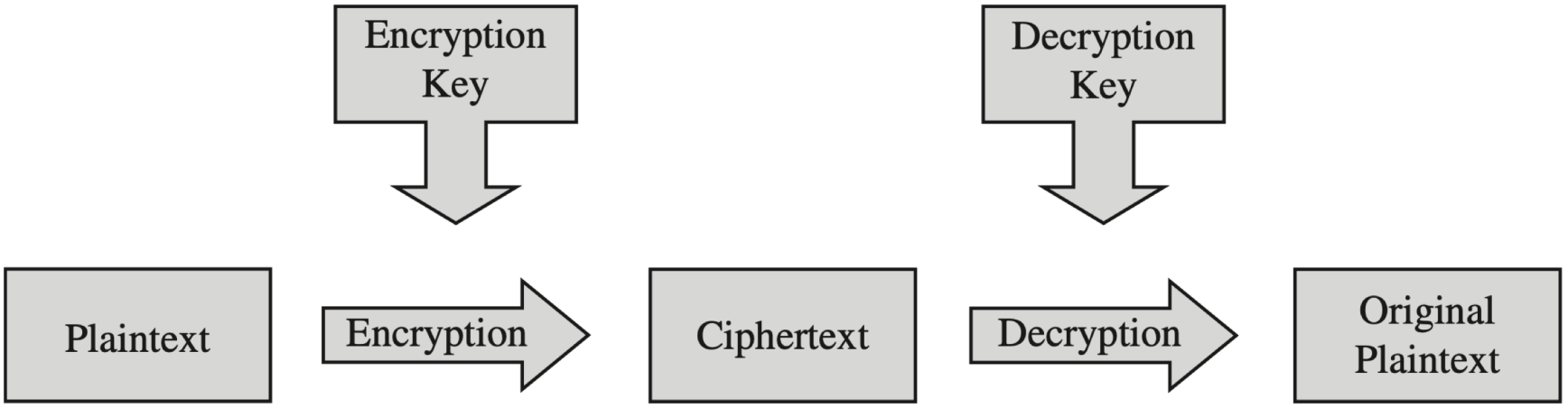
Symmetric Encryption

- Asymmetric encryption uses a pair of keys
  - Public encryption key, secret decryption key
  - A decryption key, KD, inverts the encryption of key KE, so that $P = D(KD, E(KE, P))$
  - Knowing the public KE does not betray the secret KD

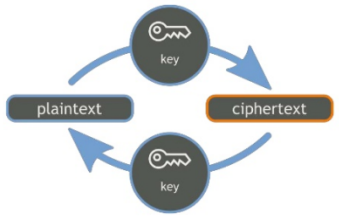
Symmetric vs. Asymmetric



(a) Symmetric Cryptosystem

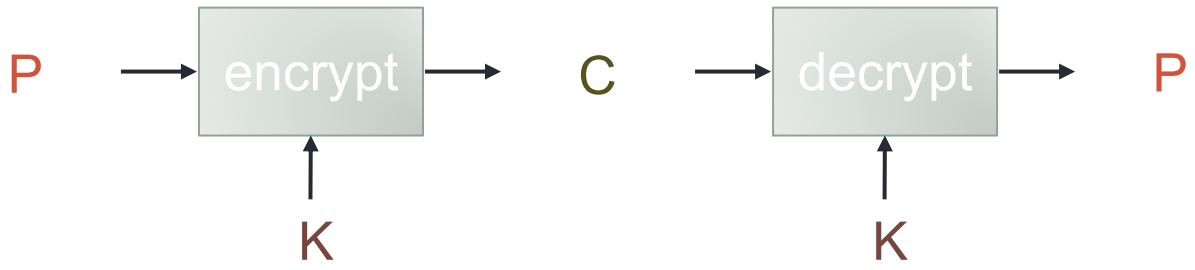


(b) Asymmetric Cryptosystem

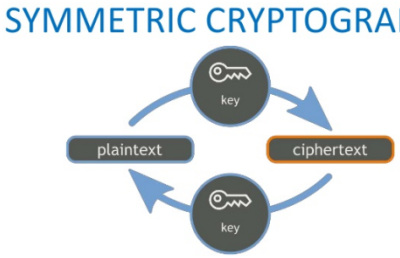


Symmetric Cryptosystem

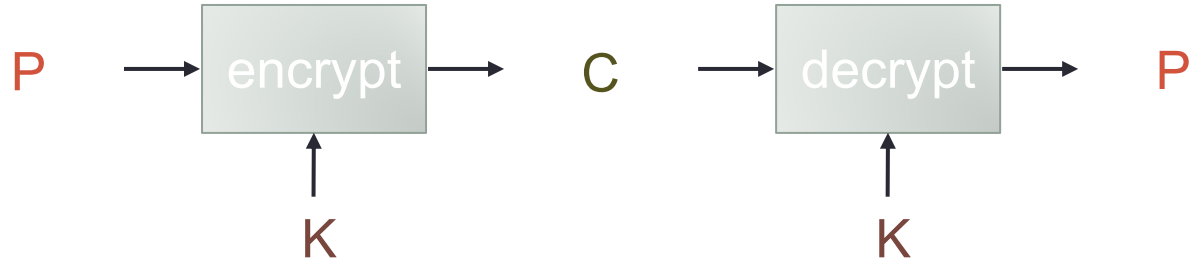
- Scenario
  - Alice wants to send a message (plaintext P) to Bob.
  - The communication channel is insecure and can be eavesdropped
  - If Alice and Bob have previously agreed on a symmetric encryption scheme and a secret key K
    - => the message can be sent encrypted (ciphertext C)



Symmetric Cryptosystem



- Issues
  - What is a good symmetric encryption scheme?
  - What is the complexity of encrypting/decrypting?
  - What is the size of the ciphertext, relative to the plaintext?



Cryptanalysis

- A cryptanalyst's goal is to break an encryption
  - Attempts to deduce the original meaning of a ciphertext message
  - Attempts to determine which decrypting algorithm, and key matches the encrypting algorithm *t*
    - to be able to break other messages encoded in the same way

Cryptanalysis

- An encryption algorithm is called ***breakable*** if:
  - it is feasible to decrypt the original message without knowing the key
    - given enough time and data
- However, an algorithm that is theoretically breakable may be impractical to break
  - May take too long (e.g. billions of years)
- The difficulty of breaking an encryption is called its ***work factor***

The Secret Keys

- ***Symmetric*** algorithms use one key, which works for both encryption and decryption
  - Usually, the decryption algorithm is closely related to the encryption one
    - running the encryption in reverse
- Both parties share a secret key
  - they can both encrypt sent information as well as decrypt information from the other

The Secret Keys

- How do two users A and B obtain their shared secret key?
  - And only A and B can use that key for their encrypted communications
  - What if A wants to share encrypted communication with another user C?
    - A and C need a different shared secret key
- Managing keys is the major difficulty in using symmetric encryption

The Secret Keys

- If we have *n* users, how many keys do we need?
  - *n* users who want to communicate in pairs need a shared key for every pair of users
    - Total of $\binom{n}{2} = \frac{n \cdot (n-1)}{2}$ keys
  - This is $O(n^2)$, the number of keys grows at a rate proportional to the square of the number of users

The Secret Keys

- If we have *n* users, how many keys do we need?
  - *n* users who want to communicate in pairs need a shared key for every pair of users
    - Total of $\binom{n}{2} = \frac{n \cdot (n-1)}{2}$ keys
  - This is $O(n^2)$, the number of keys grows at a rate proportional to the square of the number of users
- Symmetric encryption systems require a means of key distribution
- How do we solve this?

Key Exchange with TTP

- One possibility:
  - Using a Third Trusted Party (TTP)
    - Classical cryptography
- In this case, each party will have one shared secret key with the third trusted party
  - $K_a, K_b, k_c, etc.$

Key Exchange with TTP

- What A and B want to exchange a secret key:
  - TTP picks a new secret key $K_{a,b}$
  - TTP encrypts $K_{a,b}$ with K_a and sends it to A
  - TTP encrypts $K_{a,b}$ with K_b and sends it to B
  - A and B each decrypts their respective keys
    - Using their pre-shared secret key

Key Exchange with TTP

- C = Third trusted party
- C shares a secret K_a and K_b with Alice and Bob
- Key exchange protocol:
- 1. A -> C: $\{Request\ K_{a,b}\}_{K_a}$
- 2. C-> A: $\{K_{a,b}\}_{k_a}$, $\{K_{a,b}\}_{k_b}$
- 3. A-> B: $\{K_{a,b}\}_{k_b}$

Key Exchange with TTP

- Disadvantage: TTP always has to be available online to perform key exchange
- Is there another method?
  - Yes, using asymmetric encryption

Key Exchange

- ***Asymmetric or public key*** systems typically have precisely matched pairs of keys.
- The keys are produced together
  - One may be derived mathematically from the other
  - Process computes both keys as a set

Key Exchange

- Asymmetric systems good for key management
  - public key may be emailed or post it in a public directory
- Only the corresponding private key can decrypt what has been encrypted with the public key

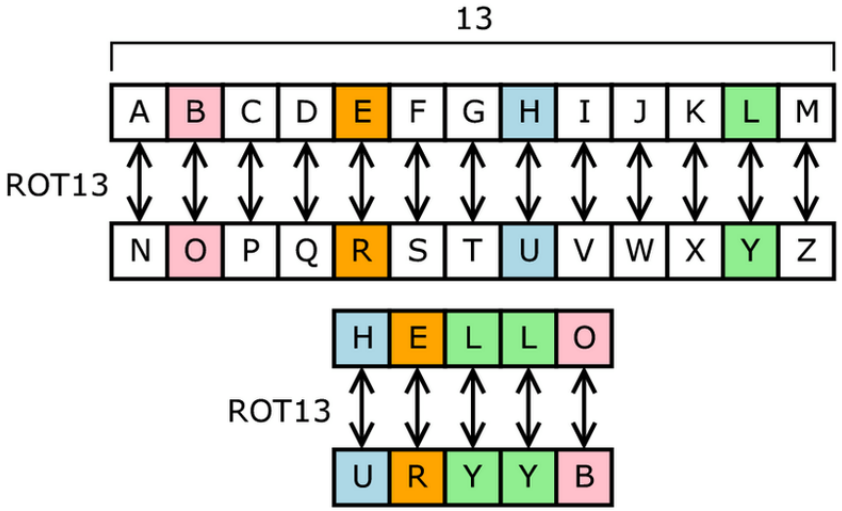
Key Exchange with Asymmetric Cryptography

- Alice chooses a pair of public and private keys K_{pb} and k_{pr}
- Alice distributes K_{pb} public key to all parties
- Bob chooses a secret key $K_{b,a}$ and encrypts it with K_{pb}
  - Sends $E(K_{b,a}, K_{pb})$ to Alice
- Alice uses her secret key K_{pr} to decrypt $K_{b,a}$
- Alice and Bob now share a secret key $K_{b,a}$

CIPHERS

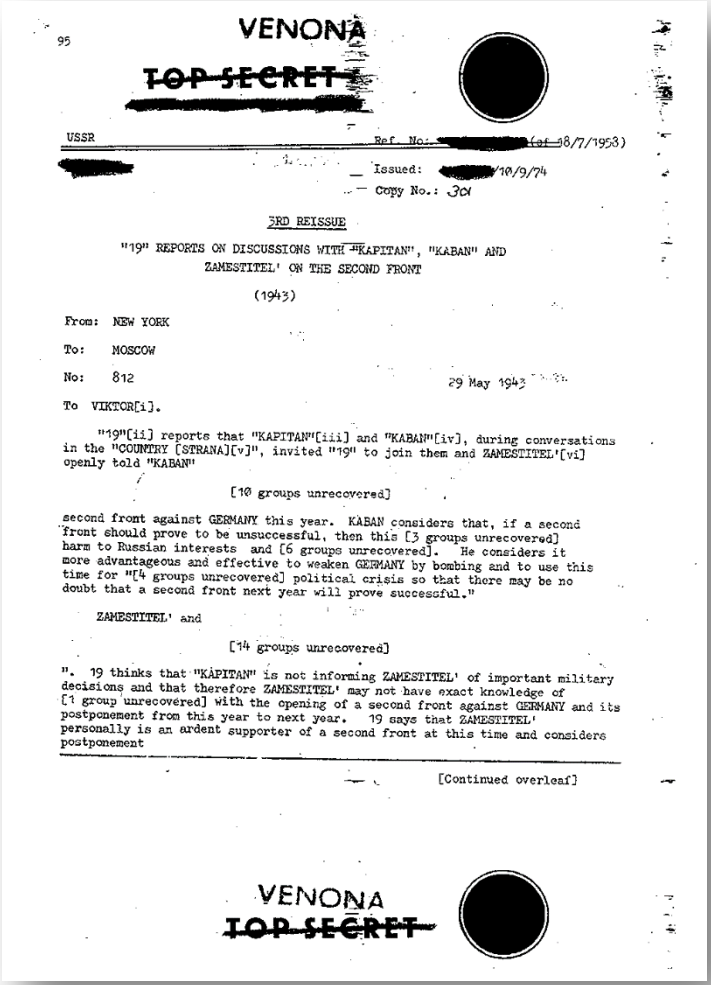
Substitution Ciphers

- Traditional ciphers, used for 1000s of years
  - Not used in modern systems anymore
- One popular substitution “cipher” for some Internet posts is ROT13.



Public domain image from http://en.wikipedia.org/wiki/File:ROT13.png

One-Time Pad



95

VENONA

~~TOP SECRET~~ [redacted]

USSR Ref. No.: [redacted] (of 8/7/1953)

[redacted] Issued: [redacted]/9/74

Copy No.: 301

3RD REISSUE

"19" REPORTS ON DISCUSSIONS WITH "KAPITAN", "KABAN" AND ZAMESTITEL' ON THE SECOND FRONT

(1943)

From: NEW YORK

To: MOSCOW

No: 812

29 May 1943

To VIKTOR[i].

"19"[ii] reports that "KAPITAN"[iii] and "KABAN"[iv], during conversations in the "COUNTRY [STRANA][v]", invited "19" to join them and ZAMESTITEL'[vi] openly told "KABAN"

[10 groups unrecovered]

second front against GERMANY this year. KABAN considers that, if a second front should prove to be unsuccessful, then this [3 groups unrecovered] harm to Russian interests and [6 groups unrecovered]. He considers it more advantageous and effective to weaken GERMANY by bombing and to use this time for "[4 groups unrecovered] political crisis so that there may be no doubt that a second front next year will prove successful."

ZAMESTITEL' and

[14 groups unrecovered]

". 19 thinks that "KAPITAN" is not informing ZAMESTITEL' of important military decisions and that therefore ZAMESTITEL' may not have exact knowledge of [1 group unrecovered] with the opening of a second front against GERMANY and its postponement from this year to next year. 19 says that ZAMESTITEL' personally is an ardent supporter of a second front at this time and considers postponement

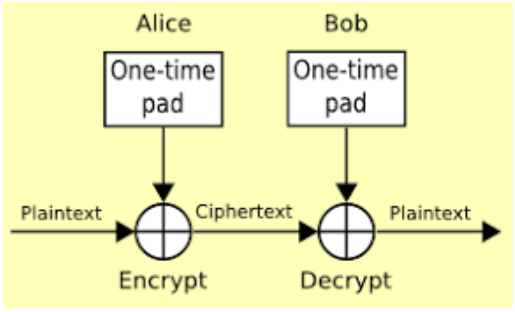
[Continued overleaf]

VENONA

~~TOP SECRET~~ [redacted]

One-Time Pads

- One variation of substitution cipher is theoretically unbreakable.
  - The one-time pad was invented in 1917 by Joseph Mauborgne and Gilbert Vernam
  - We use a block of shift keys, (k_1, k_2, . . . , k_n), to encrypt a plaintext, M, of length n
    - with each shift key being chosen uniformly at random
- Since each shift is random, every ciphertext is equally likely for any plaintext.



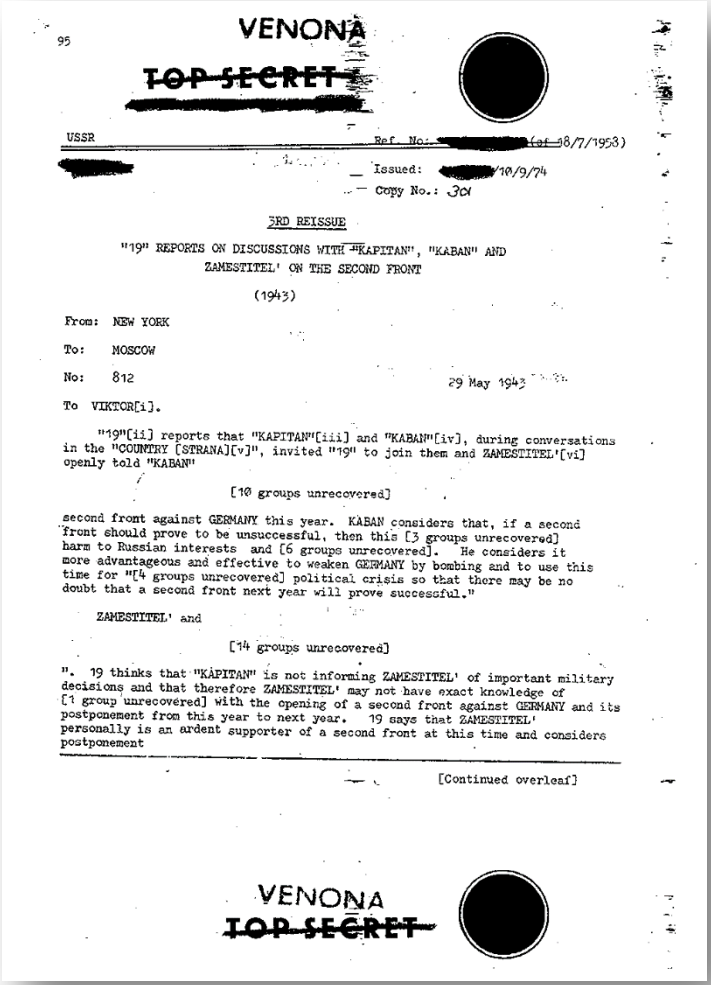
https://programmingcode4life.blogspot.com/2015/10/one-time-pad-cipher.html

Conversion Table

Conversion Table

A	= 1	K	= 11	U	= 21
B	= 2	L	= 12	V	= 22
C	= 3	M	= 13	W	= 23
D	= 4	N	= 14	X	= 24
E	= 5	O	= 15	Y	= 25
F	= 6	P	= 16	Z	= 26
G	= 7	Q	= 17		
H	= 8	R	= 18		
I	= 9	S	= 19		
J	= 10	T	= 20		

One-Time Pad



95

VENONA

~~TOP SECRET~~ [redacted]

USSR Ref. No.: [redacted] (of 8/7/1953)

[redacted] Issued: [redacted]/9/74

Copy No.: 301

3RD REISSUE

"19" REPORTS ON DISCUSSIONS WITH "KAPITAN", "KABAN" AND ZAMESTITEL' ON THE SECOND FRONT

(1943)

From: NEW YORK

To: MOSCOW

No: 812

29 May 1943

To VIKTOR[i].

"19"[ii] reports that "KAPITAN"[iii] and "KABAN"[iv], during conversations in the "COUNTRY [STRANA][v]", invited "19" to join them and ZAMESTITEL'[vi] openly told "KABAN"

[10 groups unrecovered]

second front against GERMANY this year. KABAN considers that, if a second front should prove to be unsuccessful, then this [3 groups unrecovered] harm to Russian interests and [6 groups unrecovered]. He considers it more advantageous and effective to weaken GERMANY by bombing and to use this time for "[4 groups unrecovered] political crisis so that there may be no doubt that a second front next year will prove successful."

ZAMESTITEL' and

[14 groups unrecovered]

". 19 thinks that "KAPITAN" is not informing ZAMESTITEL' of important military decisions and that therefore ZAMESTITEL' may not have exact knowledge of [1 group unrecovered] with the opening of a second front against GERMANY and its postponement from this year to next year. 19 says that ZAMESTITEL' personally is an ardent supporter of a second front at this time and considers postponement

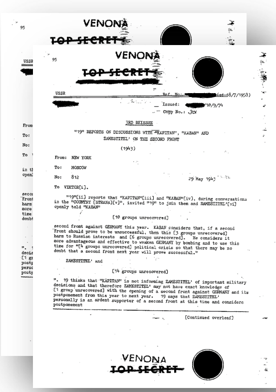
[Continued overleaf]

VENONA

~~TOP SECRET~~ [redacted]

Weaknesses of the One-Time Pad

- While perfect secure in theory, one-time pads have some weaknesses
- The key has to be as long as the plaintext
- Keys can never be reused
  - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies
    - during the Cold War.



Public domain declassified government image from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/venona-soviet-espionage-and-the-american-response-1939-1957/part2.htm

STREAM AND BLOCK CIPHER

Stream Encryption

- Each bit or byte of the data stream is encrypted separately
  - May be applicable for data stream processing

Stream Encryption

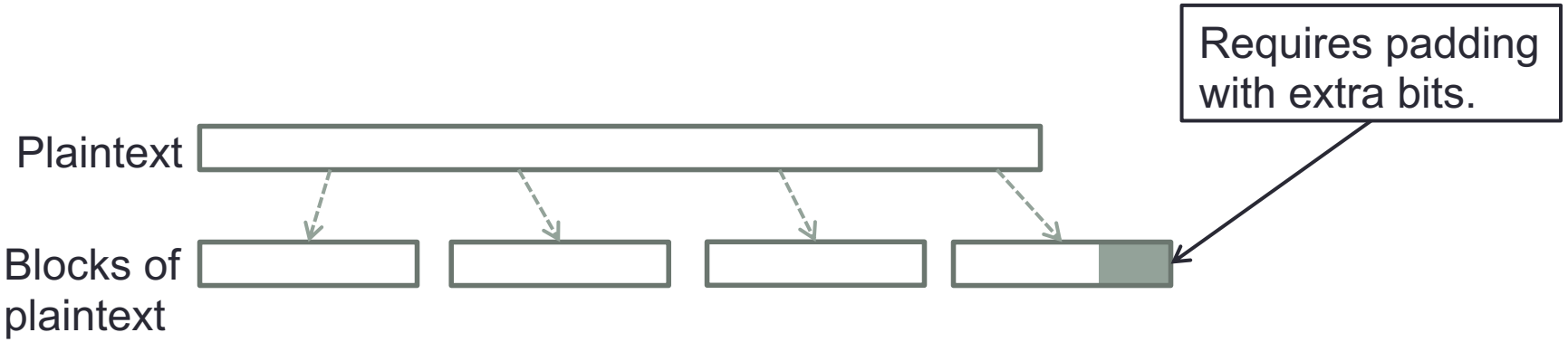
- Advantage:
  - it can be applied immediately to whatever data items are ready to transmit
- Disadvantage:
  - most encryption algorithms involve complex transformations
    - To do these transformations on one or a few bits at a time is expensive

Block Ciphers

- Perhaps the most-used technique for encryption
  - Groups plaintext symbols into fixed-size blocks
  - A block cipher algorithm performs its work on a quantity of plaintext data all at once

Block Ciphers

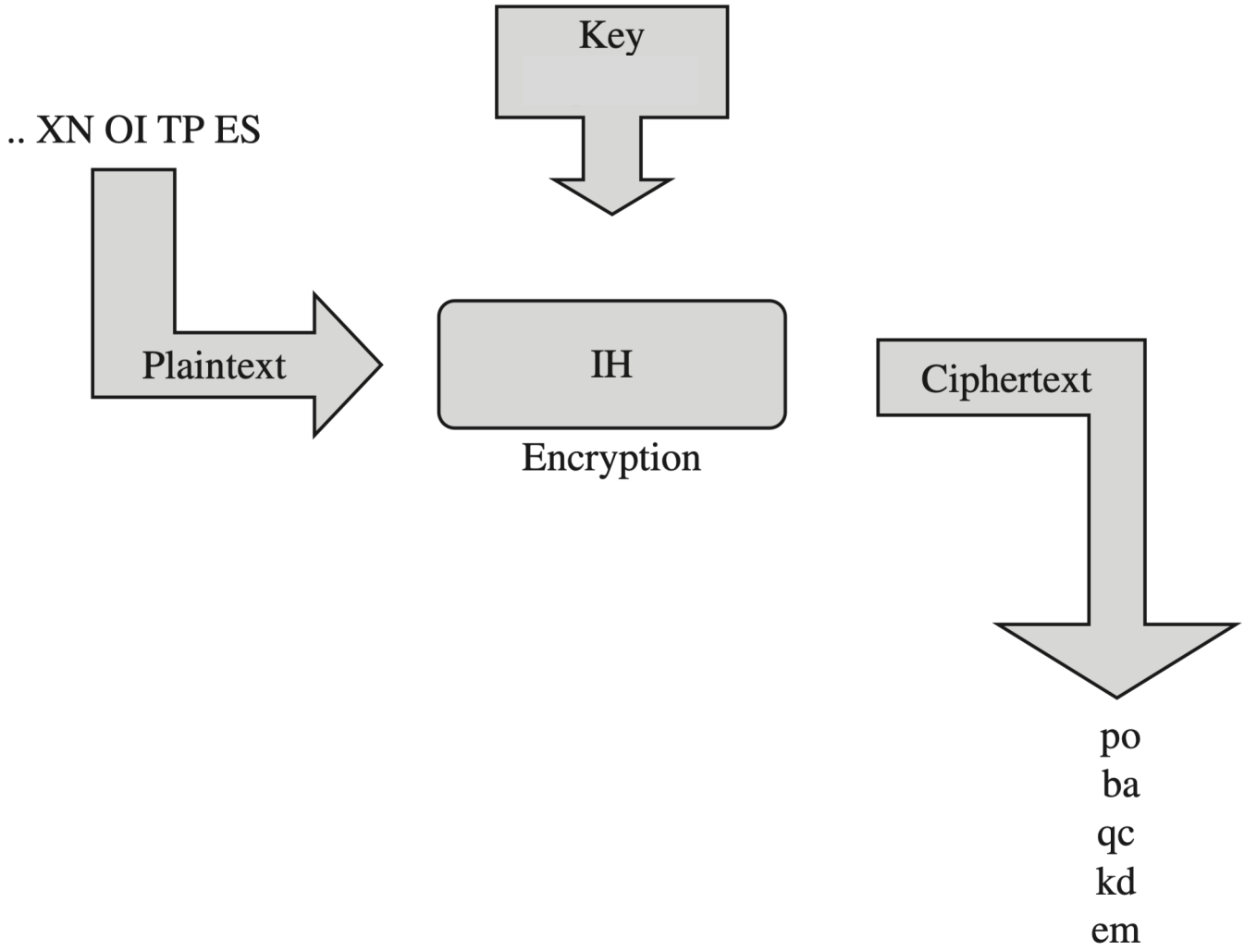
- Plaintext is partitioned into a sequence of blocks,
  - P = P[0], …, P[m–1]
- Each block is of fixed length b (e.g., 128 bits)
- Blocks encrypted (more or less) separately
  - BlockCipher(key, plaintextBlock) → ciphertextBlock



Padding

- Plaintext length must be a multiple of the block size
  - Otherwise we must pad last partial block to a full block
  - On decryption, recipient must be able to tell when data ends, padding begins
- Example for block-size = 128 (16 bytes)
  - Plaintext: “Roberto” (7 bytes)
  - Padded plaintext: “Roberto999999999” (16 bytes)
    - Problem: cannot tell if plaintext was “Roberto” or “Roberto9”
  - Better: padded plaintext “Roberto099999999”

Block Ciphers



Stream vs. Block Cipher

	Stream	Block
Encryption	Individual Chars (bits)	Groups of chars (blocks)
Speed	Faster	Slower
Hardware Circuitry	Simpler	More complex
Data Buffering	Limited or none	More space, relative to block size
Error Propagation	Limited Good for noisy channel	Faster Helps assure message integrity

www.ccs.neu.edu/home/noubir/Courses/CSG252/F04/slides4.pdf

Stream vs. Block

	Stream	Block
Advantages	• Speed of transformation • Low error propagation	• High diffusion • Immunity to insertion of symbol
Disadvantages	• Low diffusion • Susceptibility to malicious insertions and modifications	• Slowness of encryption • Padding • Error propagation

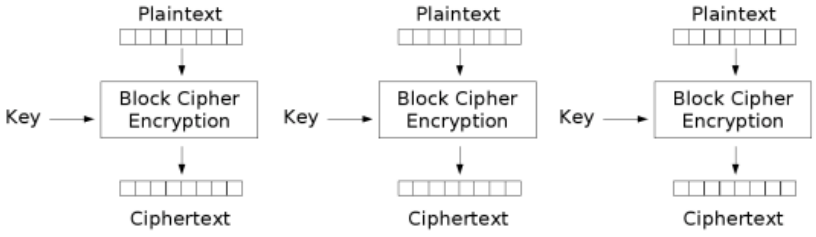
BLOCK CIPHER MODE

Block Cipher Modes

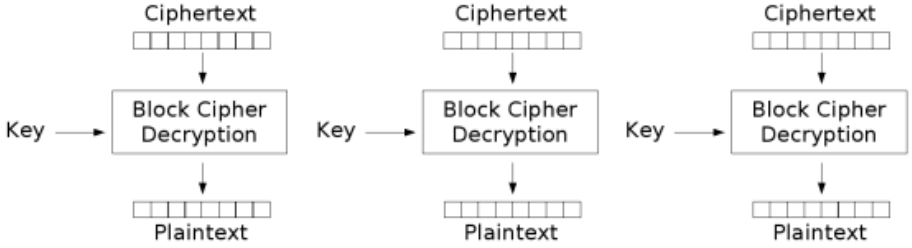
- Describe the way a block cipher encrypts and decrypts a sequence of message blocks
- Many modes exist
  - "Simple": ECB, CBC, CTR, …
  - "Authenticated": GCM, CCM, OCB, …
  - Special purpose: CMC, EME, "tweakable modes"
- We will cover ECB and CBC as examples

Electronic Code Book (ECB) Mode

- The simplest: Electronic Code Book (ECB) Mode
  - Block P[i] encrypted into ciphertext block C[i] = EK(P[i])
  - Block C[i] decrypted into plaintext block M[i] = DK(C[i])



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

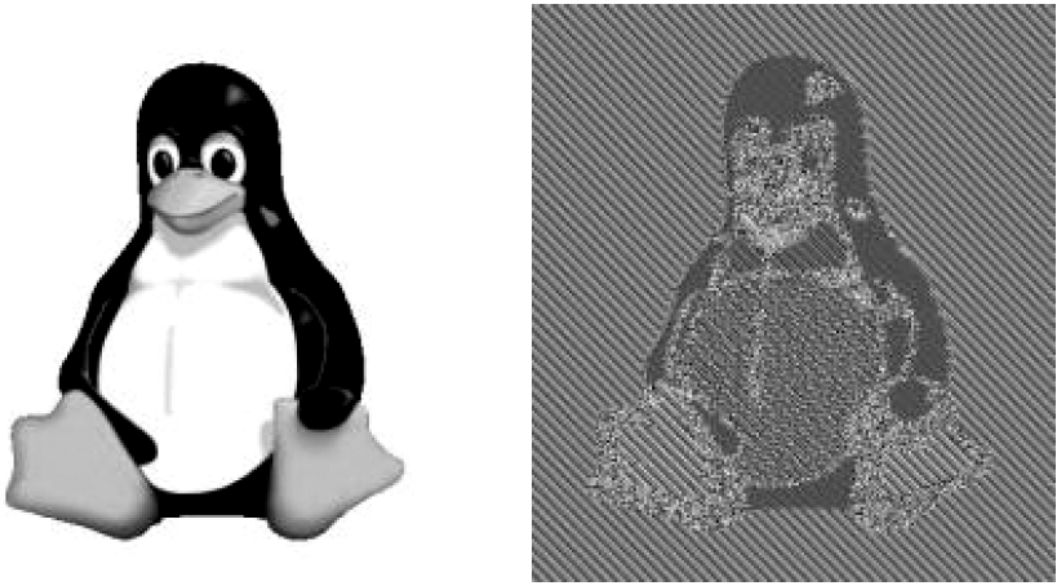
Strengths of ECB

- Very simple
- Allows for parallel encryptions of the blocks of a plaintext
- Can tolerate the loss or damage of a block

Weaknesses of ECB

- Not secure enough, patterns in the plaintext are repeated in the ciphertext
- Documents and images are not suitable for ECB encryption

Weaknesses of ECB



(a) (b)

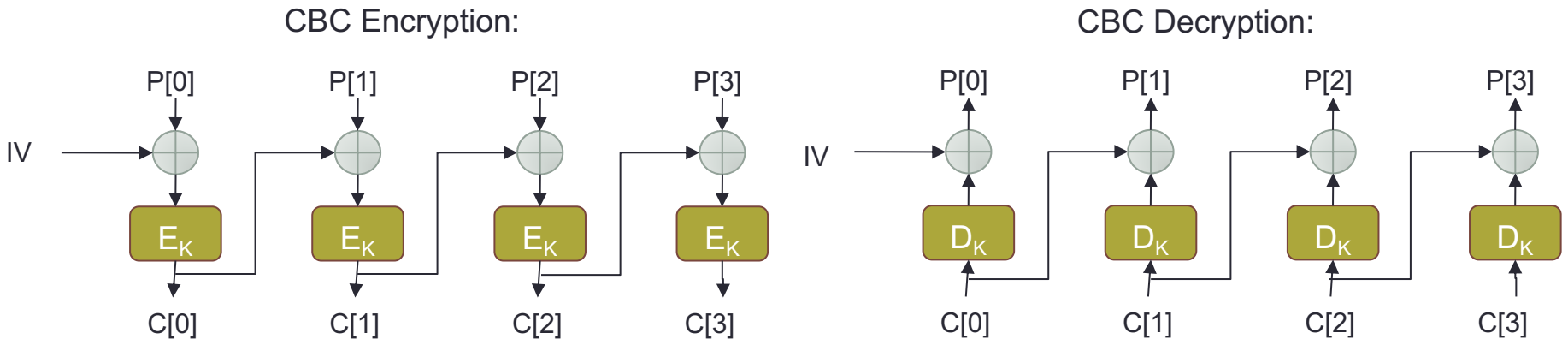
Figure 8.6: How ECB mode can leave identifiable patterns in a sequence of blocks: (a) An image of Tux the penguin, the Linux mascot. (b) An encryption of the Tux image using ECB mode. (The image in (a) is by Larry Ewing, lewing@isc.tamu.edu, using The Gimp; the image in (b) is by Dr. Juzam. Both are used with permission via attribution.)

Cipher Block Chaining (CBC) Mode

- How do we overcome this weakness?
  - Make different blocks depend on each other
  - Also use ***randomized encryption***: encrypting the same thing many times yield a different ciphertext every time

Cipher Block Chaining (CBC) Mode

- In Cipher Block Chaining (CBC) Mode
  - The previous ciphertext block is combined with the current plaintext block C[i] = EK (C[i –1] ⊕ P[i])
  - C[–1] = IV, a random block separately transmitted encrypted (known as the initialization vector)
  - Decryption: P[i] = C[i –1] ⊕ DK (C[i])



Cipher Block Chaining (CBC) Mode

- How do we overcome this weakness?
  - Make different blocks depend on each other
  - Also use randomized encryption: encrypting the same thing many times yield a different ciphertext every time

- CBC is a randomized encryption mode
  - if we choose a different iv – initial value

Strengths of CBC

- Fast and relatively simple
- Doesn’t show patterns in the plaintext
- Is the most common mode in practice
  - Usually in conjunction with an authentication method

Weaknesses of CBC

- Weaknesses:
  - Not parallelizable: encryption must be done sequentially
  - Requires reliable transmission of all the blocks sequentially
    - Not suitable for applications with packet losses (e.g., music and video streaming)
  - Still not secure enough by itself: does not provide authentication

Authentication

- Simple modes such as ECB, CBC, CTR **do not provide authentication**
  - Attacker may be able to manipulate ciphertext, inducing meaningful changes on the decrypted value
  - Some of these attacks are very sophisticated
- These modes must be used in conjunction with some other authentication mechanism
  - Providing integrity for the encrypted data

Authentication

- Some modes are specifically designed to provide both secrecy and authentication
  - E.g., GCM (Galois/Counter Mode), CCM, OCB, …

BLOCK CIPHERS IN PRACTICE

Substitution Boxes

- Substitution still used as one component (among others) in modern ciphers
- Usually applied to numbers
  - Described by substitution boxes, or S-boxes.

	00	01	10	11
00	0011	0100	1111	0001
01	1010	0110	0101	1011
10	1110	1101	0100	0010
11	0111	0000	1001	1100

(a)

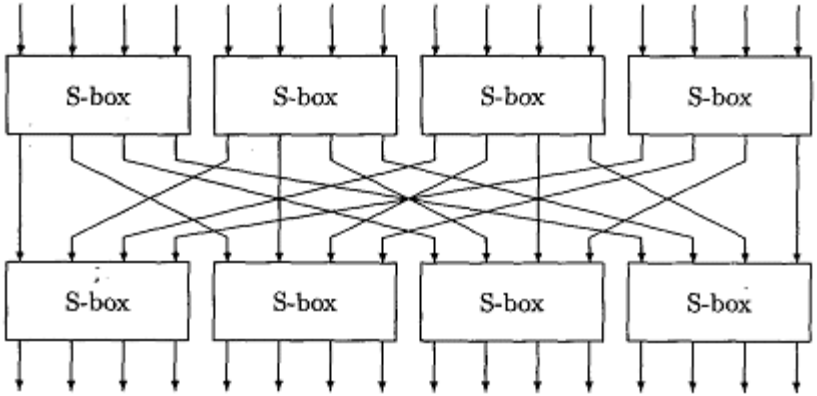
	0	1	2	3
0	3	8	15	1
1	10	6	5	11
2	14	13	4	2
3	7	0	9	12

(b)

Figure 8.3: A 4-bit S-box (a) An S-box in binary. (b) The same S-box in decimal.

Substitution Boxes

- Some modern ciphers use S-boxes that are connected to each other



https://www2.dmst.aueb.gr/dds/secimp/crypto/sp.htm

Data Encryption Standard (DES)

- Symmetric encryption algorithm
- Developed by IBM and adopted by NIST in 1977
- Encrypts 64-bit blocks using 56-bit keys
  - Relies heavily on S-boxes for securtity
- Small key space makes exhaustive search attack feasible since late 90s
  - Not secure – should not be used!

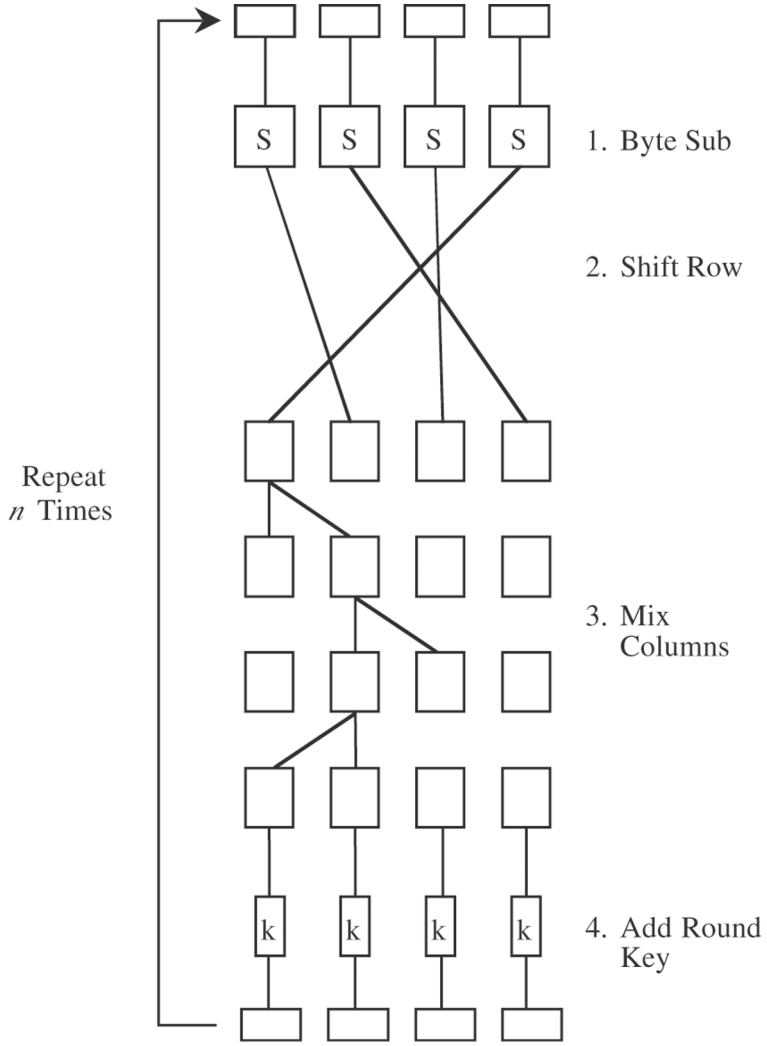
Advanced Encryption Standard (AES)

- Symmetric block cipher
- Developed in 1999 by independent Dutch cryptographers
- Selected by NIST in 2001 through open international competition and public discussion

Advanced Encryption Standard (AES)

- 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
- Exhaustive search attack not currently possible
- AES-256 is the symmetric encryption algorithm of choice
  - Still in common use

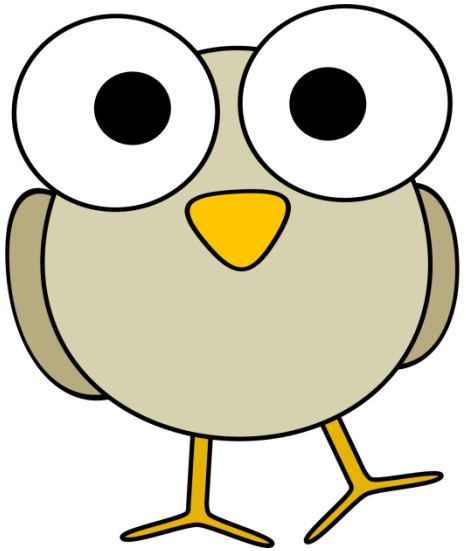
AES: Advanced Encryption System



DES vs. AES

	DES	AES
Date designed	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length); up to 112 bits with multiple keys	128, 192, 256 (and possibly more) bits
Operations	16 rounds	10, 12, 14 (depending on key length); can be increased
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but open public comments and criticisms invited
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

- Questions?



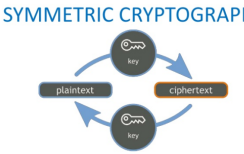
PUBLIC KEY (ASYMMETRIC) ENCRYPTION

Motivation

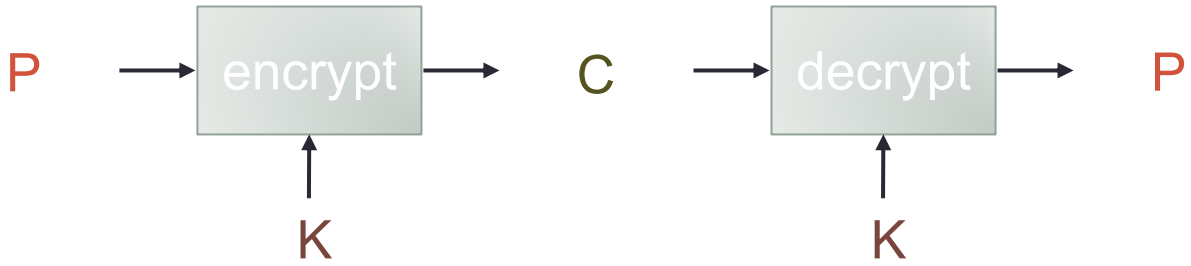
- “The basics of asymmetric cryptography are fundamental concepts that any member of society who wants to understand how the world works, or could work, needs to understand. They are as fundamental as the basics of supply and demand and monetary inflation”

Phil Libin, Evernote

Reminder - Symmetric Cryptosystem



- Scenario
  - Alice wants to send a message (plaintext P) to Bob.
  - The communication channel is insecure and can be eavesdropped
  - If Alice and Bob have previously agreed on a symmetric encryption scheme and a secret key K
    - => the message can be sent encrypted (ciphertext C)



Public Key (Asymmetric) Cryptography

- Instead of two users sharing one secret key, each user has two keys: one public and one private
- Messages encrypted using the public key can only be decrypted using the private key
  - $P = D(K_{priv}, E(K_{pub}, P))$

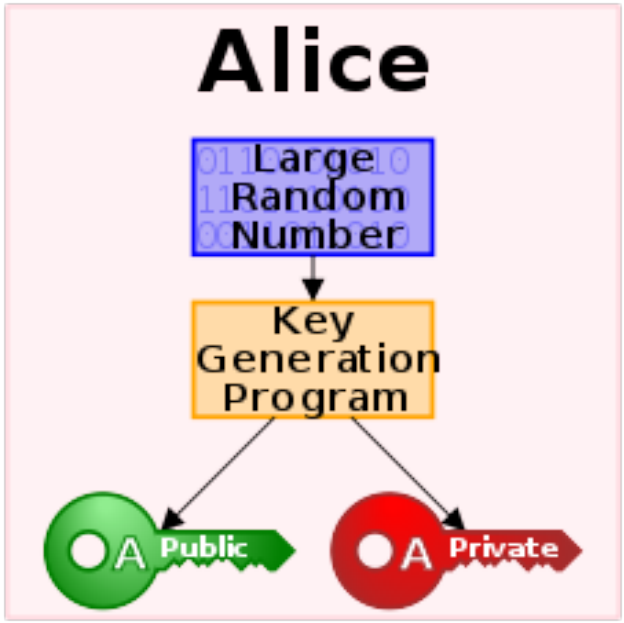
Public Key Encryption

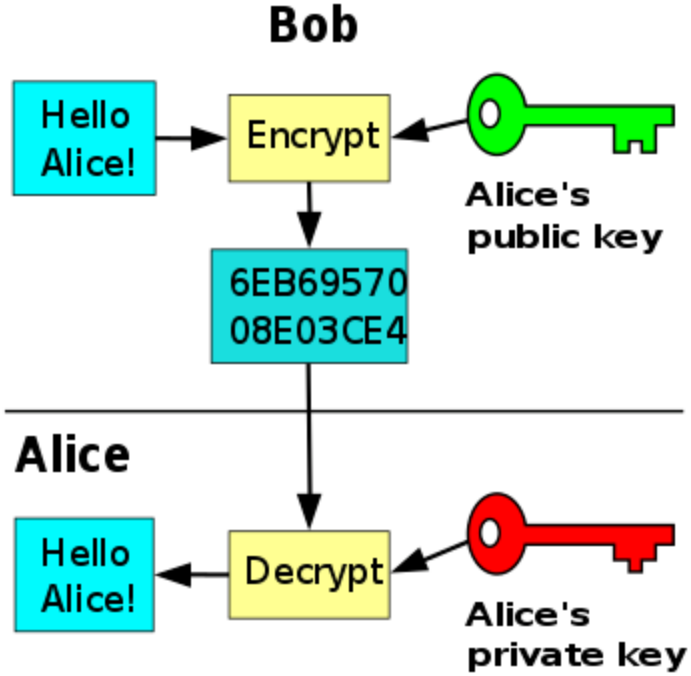
- A cryptographic system that uses pairs of keys
  - public keys which may be disseminated widely
    - Any person can encrypt the message
  - private keys which are known only to the owner
    - Message can only be decrypted with this key
- Analogous to a self-closing door
  - Need key to open it
  - Closing it shuts it automatically

Public Key Encryption

- Why does it work?
- It is not feasible to compute the private key
  - From knowledge of its paired public key
- Therefore, only the private key is kept private
  - The public key can be openly distributed without compromising security
- Public key cryptography relies on math problems that have no efficient solution

Public Key Encryption





https://en.wikipedia.org/wiki/Public-key_cryptography

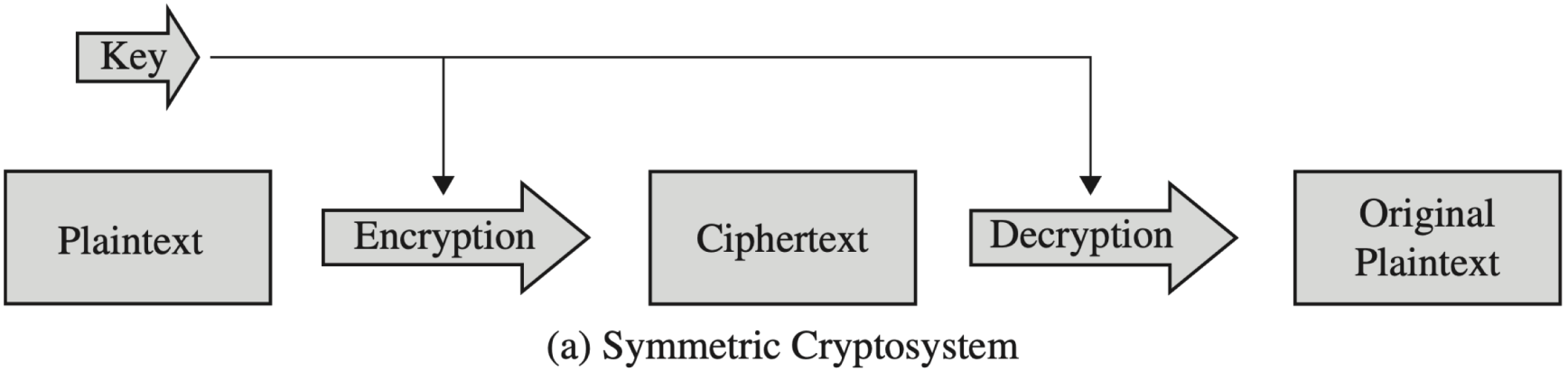
Public Key Encryption

- Often used to secure communication
  - Over the internet, open networks
  - Typically used for key exchange

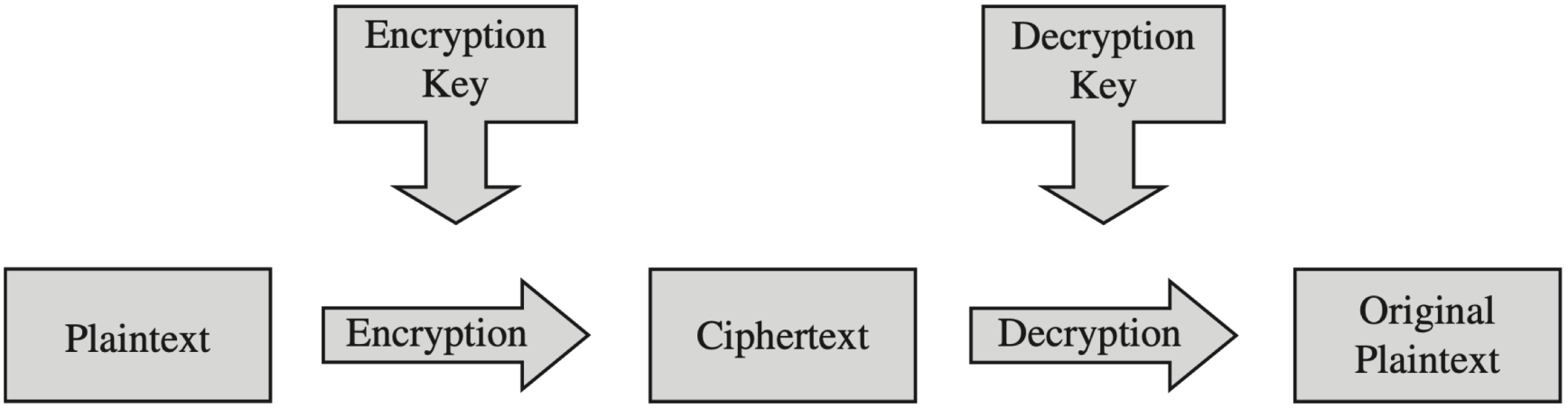
Secret Key vs. Public Key Encryption

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	56–112 (DES), 128–256 (AES)	Depending on cryptosystem, from 256 to 10000 and more
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

Symmetric vs. Asymmetric



(a) Symmetric Cryptosystem



(b) Asymmetric Cryptosystem

Symmetric vs. Asymmetric

- The critical difference between symmetric and asymmetric cryptography:
  - Symmetric uses a single key for both encryption and decryption
    - whereas asymmetric uses complementary keys

The RSA Cryptosystem (Rivest-Shamir-Adelman, 1978)

- The most widely used public-key cryptosystem
  - But becoming less popular recently
- Security relies on the hardness of the integer factorization problem
  - Given a large integer, it is costly to recover its factors
  - Makes is hard to recover secret key from public key

The RSA Cryptosystem (Rivest-Shamir-Adelman, 1978)

- Keys must be very long
  - At least 1024-bit long, usually 2048-8192
  - Because the factorization problem is not hard enough when the integers are smaller
  - Will cover it later in the course

RSA Runtime

- Keys are long: 1024-8192 bits
- Encryption is done by modular exponentiation
  - A complicated mathematical operation,

$$x, e, N \mapsto x^e mod\ N$$

  - Significantly slower that substitution, transposition that are used in symmetric encryption

- RSA runtime significantly longer than DES, AES, etc.

Secret Key vs. Public Key Encryption

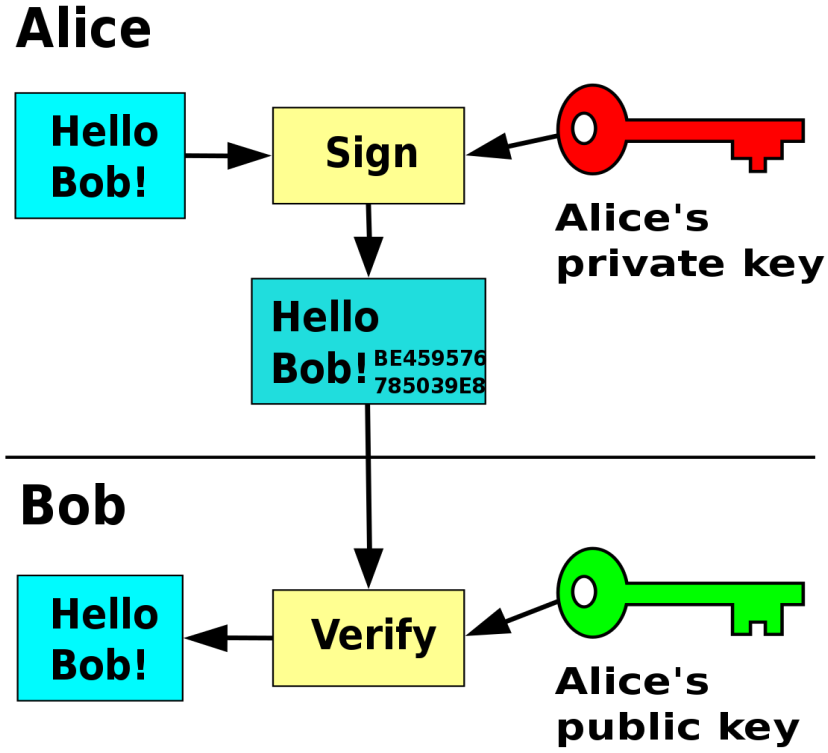
- Symmetric and asymmetric algorithms have complementary strengths and weaknesses
- Used for different purposes
  - in concert with each other

Secret Key vs. Public Key Encryption

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	56–112 (DES), 128–256 (AES)	Depending on cryptosystem, from 256 to 10000 and more
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

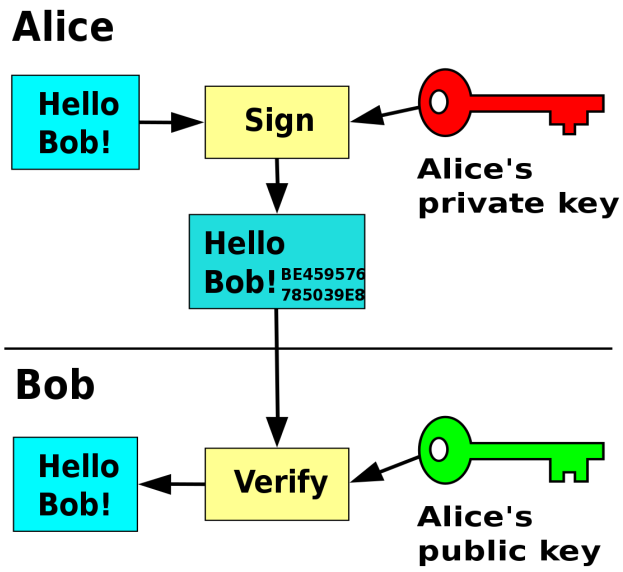
Digital Signatures

- Another use of public-key cryptosystems
- Use secret key to sign a message, public key to check validity of signature

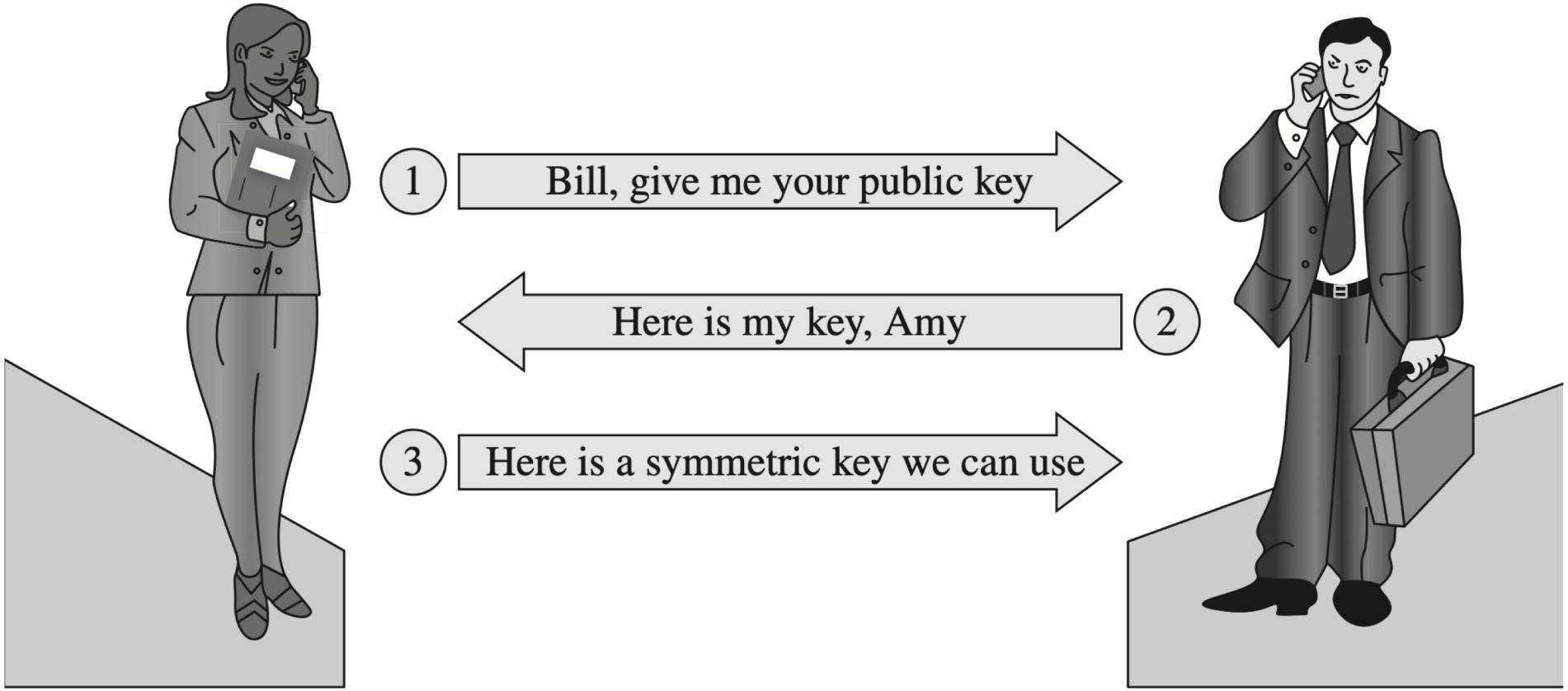


Digital Signatures

- Another use of public-key cryptosystems
- Use secret key to sign a message, public key to check validity of signature
  - People sometime mistakenly refer to signature as “decryption”



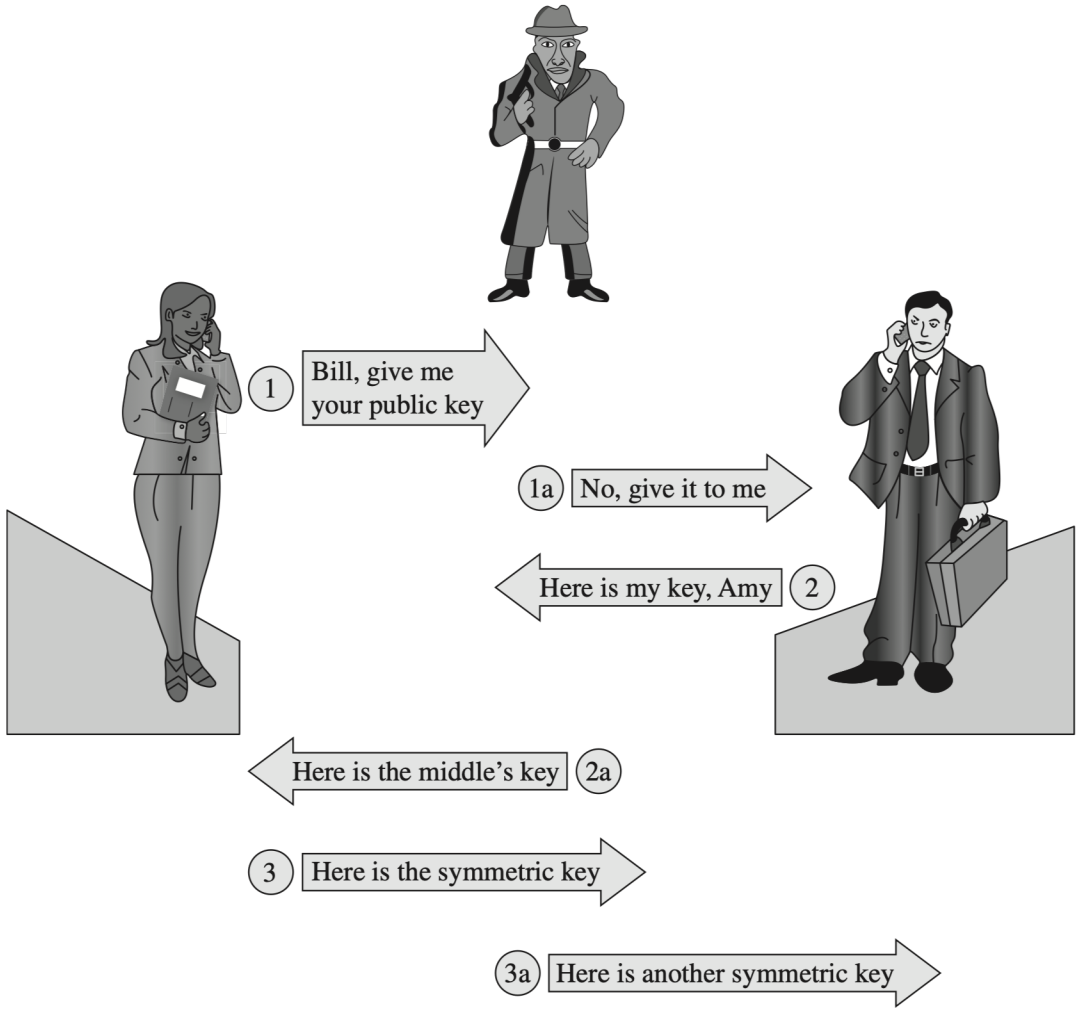
Public Key to Exchange Secret Keys



Key Exchange Man in the Middle

- What if we have a man in the middle attack?
  - Revised protocol is needed

Key Exchange Man in the Middle



Alternative Key Exchange Protocol

1. A-> B: $E(K_{pub_B}, \left(E\left(k_{priv_A}, K_S\right)\right)$ where K_S is the symmetric key

2. B uses k_{priv_B} to decrypt K_{pub_B} encryption
3. B uses K_{pub_A} to decrypt k_{priv_A} encryption and obtain K_S

Once the symmetric key has been successfully exchanged, it can be used for the rest of the communication.

Alternative Key Exchange Protocol

- Why is this more secure?
  - Only A can generate $E(k_{priv_A}, K_s)$
  - So attacker can not replace the key K_s with its own K_C
    - Such that B can decrypt it using K_{pub_A}

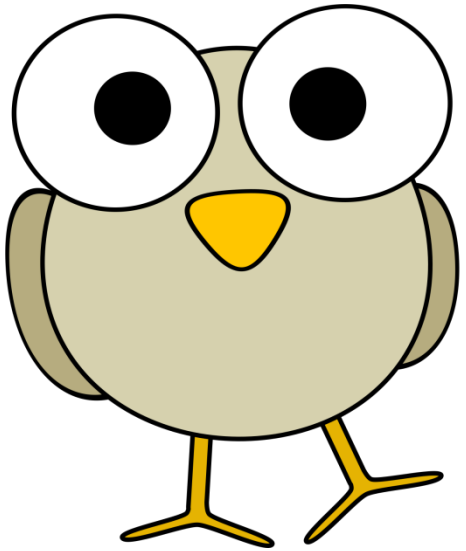
Revised Key Exchange Protocol

- Secure key exchange is complicated
- Many alternative secure protocols exist
  - Protocols need to be proven secure
  - New attacks introduced continuously

How to Break Cryptography?

- How to break cryptography

- Questions?



Error Detecting Codes

- Communications are prone to transmission errors
- Need to have a way to verify intact transmission
  - For sensitive data
- Different error detection mechanisms exist
- Aims to indicate that a message has changed
  - Different techniques work for different errors

Error Detecting vs. Correcting Codes

- ***Error detecting codes*** detect when an error has occurred
- ***Error correcting codes*** can actually correct errors without requiring a copy of the original data
  - without requiring a copy of the original data

Error Detecting vs. Correcting Codes

- The error code is computed and stored safely on the presumed intact, original data;
- Error code can be recomputed later
  - check whether the received result matches the expected value.
  - If the values do not match, a change has occurred
    - If the values match, it is probable—but not certain—that no change has occurred

Error Detecting Codes

- Demonstrates that a block of data has been modified
- Simple error detecting codes:
  - Parity checks
    - Parity bit added to a string of binary code to ensure that the total number of 1-bits in the string is even or odd
  - Cyclic redundancy checks – used on hardware devices

Error Detecting Codes

- Cryptographic error detecting codes:
  - One-way hash functions
  - Cryptographic checksums
  - Digital signatures

Parity Check

Original Data	Parity Bit	Modified Data	Modification Detected?
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 0 1	
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 0	
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 1	
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 1 1	
0 0 0 0 0 0 0 0	1	0 0 0 0 0 1 1 1	
0 0 0 0 0 0 0 0	1	0 0 0 0 1 1 1 1	
0 0 0 0 0 0 0 0	1	0 1 0 1 0 1 0 1	

Parity Check

Original Data	Parity Bit	Modified Data	Modification Detected?
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 0 1	Yes
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 0	Yes
0 0 0 0 0 0 0 0	1	1 0 0 0 0 0 0 1	No
0 0 0 0 0 0 0 0	1	0 0 0 0 0 0 1 1	No
0 0 0 0 0 0 0 0	1	0 0 0 0 0 1 1 1	Yes
0 0 0 0 0 0 0 0	1	0 0 0 0 1 1 1 1	No
0 0 0 0 0 0 0 0	1	0 1 0 1 0 1 0 1	No

Questions?