Cryptography
CS 555

Topic 1: Overview of the Course & Introduction to Encryption

See the Course Homepage

Goals of Cryptography

- The most fundamental problem cryptography addresses: ensure security of communication over insecure medium
- What does secure communication mean?
  - confidentiality (privacy, secrecy)
    - only the intended recipient can see the communication
  - integrity (authenticity)
    - the communication is generated by the alleged sender
- What does insecure medium mean?
  - Two possibilities:
    - Passive attacker: the adversary can eavesdrop
    - Active attacker: the adversary has full control over the communication channel

Approaches to Secure Communication

- Steganography
  - “covered writing”
  - hides the existence of a message
  - depends on secrecy of method
- Cryptography
  - “hidden writing”
  - hide the meaning of a message
  - depends on secrecy of a short key, not method

Terms: Cryptography, cryptanalysis, and cryptology

- Cryptography,
  - Traditionally, designing algorithms/protocols
  - Nowadays, often synonym with cryptology

- Cryptanalysis
  - Breaking algorithms/protocols

- Cryptology: both cryptography & cryptanalysis
  - Becoming less common

What Cryptography is About?

- Constructing and analyzing protocols which enables parties to achieve objectives, overcoming the influence of adversaries.
  - a protocol (or a scheme) is a suite of algorithms that tell each party what to do

- How to devise and analyze protocols
  - understand the threats posed by the adversaries and the goals

A Sample List of Other Goals in Modern Cryptography

- Modern cryptography covers many topics beyond secure communication
  - Pseudo-random number generation
  - Non-repudiation: Digital signatures
  - Zero-knowledge proof
  - Commitment schemes
  - E-voting
  - Secret sharing
  - Secure Multi-party Computation (Secure Function Evaluation)
  - …

History of Cryptography

- 2500+ years
- An ongoing battle between codemakers and codebreakers
- Driven by communication & computation technology
  - paper and ink (until end of 19^{th} century)
  - cryptographic engine & telegram, radio
    - Enigma machine, Purple machine used in WWII
  - computers & digital communication

Major Events in History of Cryptography

- Mono-alphabetical ciphers (Before 1000 AD)
- Frequency analysis (Before 1000 AD)
- Cipher machines (early 1900's)
- Shannon developed theory of perfect secrecy and information theoretical security (around 1950)
- US adopts Data Encryption Standard in 1977
- Notion of public key cryptography and digital signatures introduced (1970~1976)
- The study of cryptography becomes mainstream in the research community (1976)
- Development of computational security and other theoretical foundation of modern cryptography (1980's)

What is This Course About?

- Mostly mathematical
  - Understand the mathematics underlying the cryptographic algorithms & protocols
  - Understand the power and limitations of cryptographic tools
  - Understand the formal approach to security in modern cryptography

Backgrounds Necessary for the Course

- A bit of probability
- Algorithms and complexity
- Mathematical maturity
  - understand what is (and what is not) a proper definition
  - know how to write a proof

Symmetric-key Encryption

- This is what cryptography is all about until 1970.
- Two parties (often called a sender and a receiver) share some secret information called a key.

- Sender uses the key to encrypt (or “scramble”) the message, before it is sent
- Receiver uses the same key to decrypt (or “unscramble”) and recover the original message

Basic Terminology for Encryption

- Plaintext
  - An original message
  - Also referred to as message
- Plaintext space (aka Message space)
  - the set consisting of all possible plaintexts
- Ciphertext
  - A scrambled message
- Ciphertext space
  - The set consisting of all possible scrambled message
- Key secret used in transformation
- Key space $\mathcal{K}$

Notation for Symmetric-key Encryption

- A symmetric-key encryption scheme is comprised of three algorithms
  - **Gen** the key generation algorithm
    - The algorithm must be probabilistic/randomized
    - Output: a key *k*
  - **Enc** the encryption algorithm
    - Input: key *k*, plaintext *m*
    - Output: ciphertext c := $\mathbf{Enc}_k(m)$
  - **Dec** the decryption algorithm
    - Input: key *k*, ciphertext *c*
    - Output: plaintext m := $\mathbf{Dec}_k(m)$

Requirement: $\forall k\ \forall m\ [\ \mathbf{Dec}_k(\mathbf{Enc}_k(m)) = \mathrm{m}\ ]$

Shift Cipher

- The Key Space $\mathcal{K}$:
  - [0 .. 25]
- Encryption given a key *k*:
  - each letter in the plaintext P is replaced with the *k*'th letter following corresponding number (shift right)
- Decryption given *k*:
  - shift left

History: *k* = 3, Caesar's cipher

Shift Cipher: Cryptanalysis

- Can an attacker find K?
  - YES: by a bruteforce attack through exhaustive key search,
    - How to tell whether a shift is correct?
  - key space is small (<= 26 possible keys).

- Cipher key space needs to be large enough.
- Exhaustive key search can be effective.

Mono-alphabetic Substitution Cipher

- The key space: all permutations of Σ = {A, B, C, …, Z}
- Encryption given a key π:
  - each letter X in the plaintext P is replaced with $\pi(X)$
- Decryption given a key π:
  - each letter Y in the cipherext P is replaced with $\pi^{-1}(Y)$

Example:

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

BECAUSE $\rightarrow$ AZDBJSZ

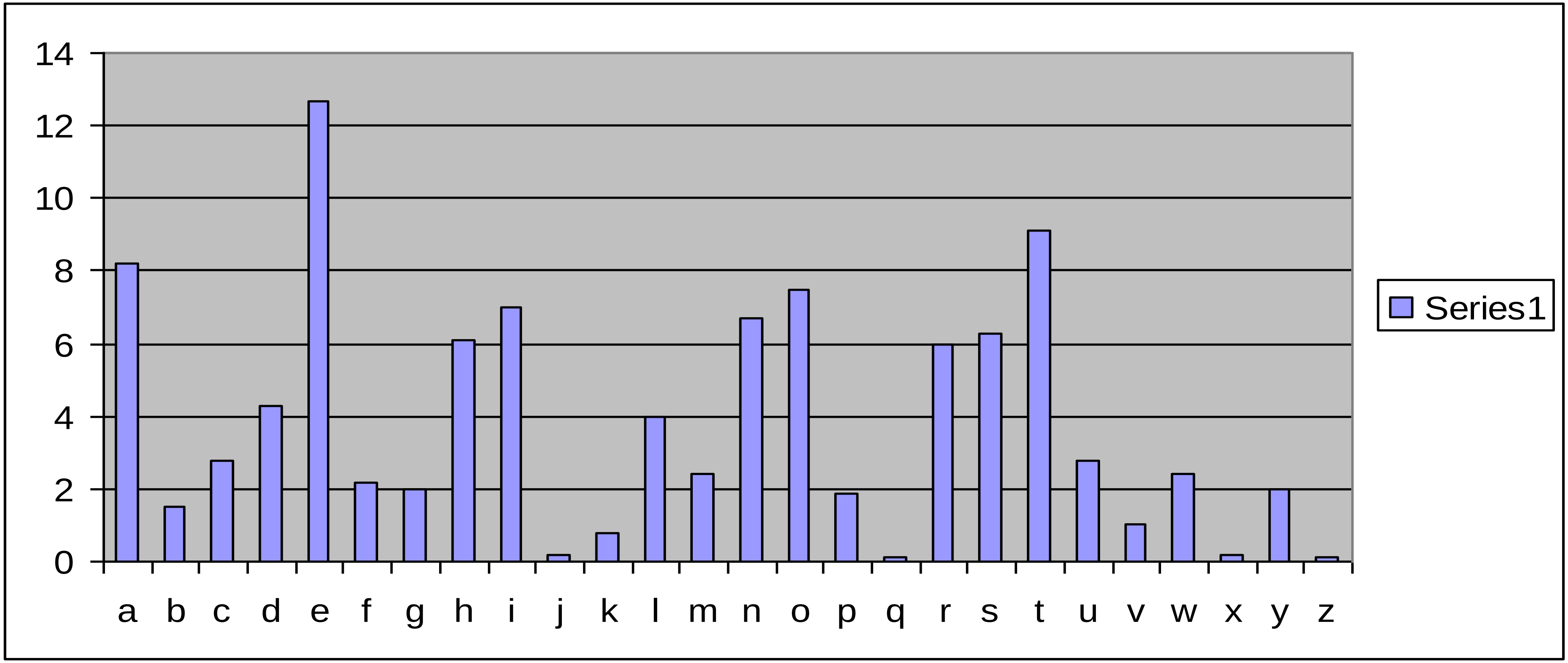
Strength of the Mono-alphabetic Substitution Cipher

- Exhaustive search is difficult
  - key space size is $26! \approx 4 \times 10^{26} \approx 2^{88}$
- Dominates the art of secret writing throughout the first millennium A.D.
- Thought to be unbreakable by many back then
- How to break it?

Cryptanalysis of Substitution Ciphers: Frequency Analysis

- Basic ideas:
  - Each language has certain features: frequency of letters, or of groups of two or more letters.
  - Substitution ciphers preserve the language features.
- History of frequency analysis
  - Discovered by the Arabs; earliest known description is in a book by the ninth-century scientist al-Kindi
  - Rediscovered or introduced from the Arabs in the Europe during the Renaissance
- Frequency analysis made substitution cipher insecure

Frequency of Letters in English



How to Defeat Frequency Analysis?

- Use larger blocks as the basis of substitution. Rather than substituting one letter at a time, substitute 64 bits at a time, or 128 bits.
  - Leads to block ciphers such as DES & AES.

- Use different substitutions to get rid of frequency features.
  - Leads to polyalphabetical substituion ciphers, cipher machines, and stream ciphers

Coming Attractions …

- Vigenere cipher.

- Required reading
  - Katz and Lindell: 1.1 to 1.3

- Recommended reading
  - The Code Book: Chapters 1 to 4