Cryptology Part 1

Charles Abzug, Ph.D.
Department of Computer Science
James Madison University
Harrisonburg, VA 22807

Voice Phone: *540-568-8746;* Cell Phone: *443-956-9424*
E-mail: *abzugcx@JMU.edu* OR *CharlesAbzug@ACM.org*
Home Page: *http://www.cs.jmu.edu/users/abzugcx*

© 2004 Charles Abzug

Uses of Cryptology

1. Transmission of a message with assurance that the contents will be known only by sender and recipient
   a) Steganography: existence of the message is hidden
   b) Cryptography: garbling of the message so that its meaning can be discerned only by the intended recipient
      i. Codes
      ii. Ciphers
2. Authentication
   a) Message content
   b) Message origin (Digital Signature)
3. Miscellaneous other uses and issues
   a) Electronic Voting: Confirmation of Voter-ID, Prevention of Double-Voting, Maintenance of Anonymity
   b) Signing of Contracts: Simultaneity
   c) E-cash: Avoidance of Fraud, Maintenance of Anonymity, Prevention of Tax-Avoidance
   d) Zero-Knowledge Protocol: ability of one party to convince the other that he/she has a secret, without revealing what it is

Terminology

1. Code
2. Cipher
3. Key
4. Algorithm
5. Plaintext (or Cleartext)
6. Ciphertext
7. Steganography
8. Cryptology
9. Cryptography
10. Cryptanalysis
11. Enciphering or Encrypting
12. Deciphering or Decrypting
13. Etymology: κρψπoσ (kryptos) λογοσ (logos) γραφια (graphia)
14. Passive Attack
15. Active Attack
16. Symmetric (classical cryptography , as well as modern)
17. Asymmetric (modern only)

Basic Approaches to Cryptography

1. Transposition: e.g., the Spartan *Scytale* (pronunciation: SIT-a-lee)
2. Substitution: most modern ciphers

Basic Approaches to Cryptography: (1) Transposition

SYBLCRESEERACHTAYPUOHIPHRUEMTYILSOOITDOFG

S B C E E R C T Y U H P R E T I S O T O G
Y I R S E A H A P O I H U M Y L O ! D F

S L E E C A U I R M I O T F
Y C S R H Y O P U T L O D G
B R E A T P H H E Y S ! O

S C E C Y H R T S T G
Y R E H P I U Y O D
B E R T U P E I O O
L S A A O H M L ! F

S R R A H U I ! G
Y E A Y I E L T
B S C P P M S D
L E H U H T O O
C E T O R Y O F

Basic Approaches to Cryptography: (1) Transposition (continued)

SYBLCRESEERACHTAYPUOHIPHRUEMTYILSOOITDOFG

S E C U R I T
Y S H O U L D
B E T H E S O
L E A I M O F
C R Y P T O G
R A P H Y !

Simple Additive Cipher

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

cleartext → .

OHWWHU → .

Simple Additive Cipher

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

cleartext → FOHDUWHAW

OHWWHU → letter

Basic Approaches to Cryptography: (2) Substitution

1. Monoalphabetic Ciphers over the "natural" alphabet
   a) Additive Ciphers or Shift Ciphers (keys: 1, 2, , , 25; keyspace = ?)
   b) Multiplicative Ciphers (keys: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25; keyspace = ?)
   c) Affine Ciphers (keyspace = ?)
   d) General Monoalphabetic Cipher (keyspace = ?)

Basic Approaches to Cryptography: (2) Substitution

1. Monoalphabetic Ciphers over the "natural" alphabet
   a) Additive Ciphers or Shift Ciphers (keys: 1, 2, , , 25; keyspace = 26)
   b) Multiplicative Ciphers (keys: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25; keyspace = 12)
   c) Affine Ciphers (keyspace = ???)
   d) General Monoalphabetic Cipher (keyspace = ?)

Basic Approaches to Cryptography: (2) Substitution

1. Monoalphabetic Ciphers over the "natural" alphabet
   a) Additive Ciphers or Shift Ciphers (keys: 1, 2, , , 25; keyspace = 26)
   b) Multiplicative Ciphers (keys: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25; keyspace = 12)
   c) Affine Ciphers (keyspace = 12 * 26 = 312)
   d) General Monoalphabetic Cipher (keyspace = ???)

Susceptibility of Monoalphabetic Ciphers to Cryptanalysis

1. "Brute Force" Attack: try all possible keys
2. Frequency Analysis (al-Kindi, eighth century)

Relative Frequencies of Letters in English Text

letter	Relative Frequency (%)		letter	Relative Frequency (%)
a	8.167		n	6.749
b	1.492		o	7.507
c	2.782		p	1.929
d	4.253		q	0.095
e	12.702		r	5.987
f	2.228		s	6.327
g	2.015		t	9.056
h	6.094		u	2.758
i	6.966		v	0.978
j	0.153		w	2.360
k	0.772		x	0.150
l	4.025		y	1.974
m	2.406		z	0.074

© 2004 Charles Abzug

Basic Approaches to Cryptography: (2) Substitution

1. Monoalphabetic Ciphers over the "natural" alphabet
   a) Additive Ciphers or Shift Ciphers (keys: 1, 2, , , 25; keyspace = 26)
   b) Multiplicative Ciphers (keys: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25; keyspace = 12)
   c) Affine Ciphers (keyspace = 12 * 26 = 312)
   d) General Monoalphabetic Cipher (keyspace = 26! = 403,291,461,126,605,635,584,000,000 > 4 * 10^{26})
2. Polyalphabetic Ciphers over the "natural" alphabet
3. Complex Monoalphabetic Ciphers

© 2004 Charles Abzug

Simple Monoalphabetic Cipher with Keyword

1. Uses a keyword
2. Second and all subsequent repetitions of each character deleted
3. Length of keyword generally smaller than 26
4. Remaining letters of alphabet (i.e., those not present in the keyword) then listed in alphabetical order to make up 26 letters.
5. Example keyword: ANTIDISESTABLISHMENTARIANISM
6. Example keyword with duplicates removed: ANTIDSEBLHMNR
7. Final key, augmented from keyword: ANTIDSEBLHMNRCFGJKOPQUVWXYZ

© 2004 Charles Abzug

Polyalphabetic Cipher with Keyword: the Vigenère Cipher

1. Uses a keyword
2. Second and all subsequent repetitions of each character deleted
3. Length of keyword generally smaller than 26
4. Keyword repeated as many times as necessary to fill out the plaintext
5. Each letter of plaintext encrypted IAW the corresponding line of the Vigenère square)
6. Example keyword: ANTIDISESTABLISHMENTARIANISM
7. Example keyword with duplicates removed: ANTIDSEBLHMNR
8. Final Key: ANTIDSEBLHMNRANTIDSEBLHMNRANTIDSEBLHMNRANTIDSEBLHMNRANTIDSEBLHMNRANTIDSEBLHMNR . . .
9. Keyword Length for this example: 13

© 2004 Charles Abzug

More Robust Polyalphabetic Cipher with Keytext

1. Uses a lengthy text as key
2. Repetitions of key characters accepted
3. Arbitrary length of key text: generally longer than plaintext
4. Each letter of plaintext encrypted IAW the corresponding line of the Vigenère square)
5. Example key text: WHEN IN THE COURSE OF HUMAN EVENTS IT BECOMES NECESSARY FOR ONE PEOPLE TO DISSOLVE THE POLITICAL BANDS WHICH HAVE CONNECTED THEM WITH ANOTHER AND TO ASSUME AMONG THE POWERS OF THE EARTH THE SEPARATE AND EQUAL STATION TO WHICH THE LAWS OF NATURE AND . . .

© 2004 Charles Abzug

Attacks on Vigenère Cipher

1. Overall strategy: Determine the keylength; once known, the problem reduces to multiple monoalphabetic substitutions.
2. By hand: search for repeating digraphs, trigraphs, quadgraphs to guess keylength.
3. Develop table of repetition distances for each character pattern.

© 2004 Charles Abzug

Stallings' Fig. 3.5

Stallings' Fig. 3.6

Stallings' Fig. 3.7

Stallings' Fig. 3.8

Stallings' Fig. 3.9

Needham-Schroeder Protocol

- original third-party key distribution protocol
- for session between A & B mediated by KDC
- protocol overview is:
  1. $A \rightarrow KDC$: $ID_A \,||\, ID_B \,||\, N_1$
  2. $KDC \rightarrow A$: $E_{Ka}[Ks \,||\, ID_B \,||\, N_1 \,||\, E_{Kb}[Ks||ID_A]\,]$
  3. $A \rightarrow B$: $E_{Kb}[Ks||ID_A]$
  4. $B \rightarrow A$: $E_{Ks}[N_2]$
  5. $A \rightarrow B$: $E_{Ks}[f(N_2)]$

Needham-Schroeder Protocol

- used to securely distribute a new session key for communications between A & B
- but is vulnerable to a replay attack if an old session key has been compromised
  - then message 3 can be resent convincing B that is communicating with A
- modifications to address this require:
  - timestamps (Denning 81)
  - using an extra nonce (Neuman 93)

Using Public-Key Encryption

- have a range of approaches based on the use of public-key encryption
- need to ensure have correct public keys for other parties
- using a central Authentication Server (AS)
- various protocols exist using timestamps or nonces

Denning AS Protocol

- Denning 81 presented the following:
  1. $A \rightarrow AS$: $ID_A \,||\, ID_B$
  2. $AS \rightarrow A$: $E_{KRas}[ID_A||KU_a||T] \,||\, E_{KRas}[ID_B||KU_b||T]$
  3. $A \rightarrow B$: $E_{KRas}[ID_A||KU_a||T] \,||\, E_{KRas}[ID_B||KU_b||T] \,||\, E_{KUb}[E_{KRas}[K_s||T]]$
- note session key is chosen by A, hence AS need not be trusted to protect it
- timestamps prevent replay but require synchronized clocks

One-Way Authentication

- required when sender & receiver are not in communications at same time (eg. email)
- have header in clear so can be delivered by email system
- may want contents of body protected & sender authenticated

Using Symmetric Encryption

- can refine use of KDC but can't have final exchange of nonces, vis:
  1. $A \rightarrow KDC$: $ID_A \,||\, ID_B \,||\, N_1$
  2. $KDC \rightarrow A$: $E_{Ka}[Ks \,||\, ID_B \,||\, N_1 \,||\, E_{Kb}[Ks||ID_A]\,]$
  3. $A \rightarrow B$: $E_{Kb}[Ks||ID_A] \,||\, E_{Ks}[M]$
- does not protect against replays
  - could rely on timestamp in message, though email delays make this problematic

Public-Key Approaches

- have seen some public-key approaches
- if confidentiality is major concern, can use:
  $A \rightarrow B$: $E_{KUb}[Ks] \,||\, E_{Ks}[M]$
  - has encrypted session key, encrypted message
- if authentication needed use a digital signature with a digital certificate:
  $A \rightarrow B$: $M \,||\, E_{KRa}[H(M)] \,||\, E_{KRas}[T||ID_A||KU_a]$
  - with message, signature, certificate

Arbitrated Techniques for Digital Signature

Stallings' Table 13.1

© 2004 Charles Abzug

Kerberos

- trusted key server system from MIT
- provides centralised private-key third-party authentication in a distributed network
  - allows users access to services distributed through network
  - without needing to trust all workstations
  - rather all trust a central authentication server
- two versions in use: 4 & 5

© 2004 Charles Abzug

Kerberos Requirements

- first published report identified its requirements as:
  - security
  - reliability
  - transparency
  - scalability
- implemented using an authentication protocol based on Needham-Schroeder

© 2004 Charles Abzug

Kerberos 4 Overview

- a basic third-party authentication scheme
- have an Authentication Server (AS)
  - users initially negotiate with AS to identify self
  - AS provides a non-corruptible authentication credential (ticket granting ticket TGT)
- have a Ticket Granting server (TGS)
  - users subsequently request access to other services from TGS on basis of users TGT

© 2004 Charles Abzug

Kerberos 4 Overview

Stallings' Fig. 14.1

© 2004 Charles Abzug

Message Exchanges in Kerberos v.4

Stallings' Table 14.3

© 2004 Charles Abzug

Kerberos Realms

- a Kerberos environment consists of:
  - a Kerberos server
  - a number of clients, all registered with server
  - application servers, sharing keys with server
- this is termed a realm
  - typically a single administrative domain
- if have multiple realms, their Kerberos servers must share keys and trust

Kerberos Version 5

- developed in mid 1990's
- provides improvements over v4
  - addresses environmental shortcomings
    - encryption alg, network protocol, byte order, ticket lifetime, authentication forwarding, interrealm auth
  - and technical deficiencies
    - double encryption, non-std mode of use, session keys, password attacks
- specified as Internet standard RFC 1510

X.509 Authentication Service

- part of CCITT X.500 directory service standards
  - distributed servers maintaining some info database
- defines framework for authentication services
  - directory may store public-key certificates
  - with public key of user
  - signed by certification authority
- also defines authentication protocols
- uses public-key crypto & digital signatures
  - algorithms not standardised, but RSA recommended

X.509 Certificates

- issued by a Certification Authority (CA), containing:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (of hash of all fields in certificate)
- notation CA<<A>> denotes certificate for A signed by CA

X.509 Certificates

Stallings' Fig. 14.3

Obtaining a Certificate

- any user with access to CA can get any certificate from it
- only the CA can modify a certificate
- because cannot be forged, certificates can be placed in a public directory

CA Hierarchy

- if both users share a common CA then they are assumed to know its public key
- otherwise CA's must form a hierarchy
- use certificates linking members of hierarchy to validate other CA's
  - each CA has certificates for clients (forward) and parent (backward)
- each client trusts parents certificates
- enable verification of any certificate from one CA by users of all other CAs in hierarchy

© 2004 Charles Abzug

CA Hierarchy Use

Stallings' Fig 14.4

© 2004 Charles Abzug

Certificate Revocation

- certificates have a period of validity
- may need to revoke before expiry, eg:
  1. user's private key is compromised
  2. user is no longer certified by this CA
  3. CA's certificate is compromised
- CA's maintain list of revoked certificates
  - the Certificate Revocation List (CRL)
- users should check certs with CA's CRL

© 2004 Charles Abzug

Authentication Procedures

- X.509 includes three alternative authentication procedures:
- One-Way Authentication
- Two-Way Authentication
- Three-Way Authentication
- all use public-key signatures

© 2004 Charles Abzug

One-Way Authentication

- 1 message (A->B) used to establish
  - the identity of A and that message is from A
  - message was intended for B
  - integrity & originality of message
- message must include timestamp, nonce, B's identity and is signed by A

© 2004 Charles Abzug

Two-Way Authentication

- 2 messages (A->B, B->A) which also establishes in addition:
  - the identity of B and that reply is from B
  - that reply is intended for A
  - integrity & originality of reply
- reply includes original nonce from A, also timestamp and nonce from B

© 2004 Charles Abzug

Three-Way Authentication

- 3 messages (A->B, B->A, A->B) which enables above authentication without synchronized clocks
- has reply from A back to B containing signed copy of nonce from B
- means that timestamps need not be checked or relied upon

© 2004 Charles Abzug

X.509 Version 3

- has been recognised that additional information is needed in a certificate
  - email/URL, policy details, usage constraints
- rather than explicitly naming new fields defined a general extension method
- extensions consist of:
  - extension identifier
  - criticality indicator
  - extension value

© 2004 Charles Abzug

Certificate Extensions

- key and policy information
  - convey info about subject & issuer keys, plus indicators of certificate policy
- certificate subject and issuer attributes
  - support alternative names, in alternative formats for certificate subject and/or issuer
- certificate path constraints
  - allow constraints on use of certificates by other CA's

© 2004 Charles Abzug

Summary

- have considered:
  - Kerberos trusted key server system
  - X.509 authentication and certificates

© 2004 Charles Abzug

Data Encryption Standard (DES)

© 2004 Charles Abzug

Stallings' Fig. 3.5

© 2004 Charles Abzug

Stallings' Fig. 3.6

Stallings' Fig. 3.7

Stallings' Table 3.2

Stallings' Fig. 3.8

Stallings' Fig. 3.9

Stallings' Table 3.3

Stallings' Table 3.4

Stallings' Table 3.5

Stallings' Fig. 3.15

Advanced Encryption Standard (AES)

Stallings' Table 5.3

Stallings' Fig. 5.1

Stallings' Fig. 5.2

Stallings' Fig. 5.3

Stallings' Fig. 5.7

END