CS 578 – Cryptography

Prof. Michael Backes

Logistics and Historical Ciphers

April 21, 2006

Organization

- CS 578 – Introduction to Cryptography
- http://infsec.cs.uni-sb.de/teaching/SS06/vorlesung_s06.html
- Teaching assistants:
  - Michaela Götz, Dirk Heine, Esfandiar Mohammadi
  - cs578@mail-infsec.cs.uni-sb.de
- Tutor Office Hours (in E 1 1, U 19)
  - Wed 9-11, Thu 14-16, Fri 14-16
- Practical classes:
  - Wednesday 2 x 1-2pm, 4-5pm
- Registration
  - Opens today, link on course web page

Organization (cont'd)

- Weekly homework exercises
  - Handed out Tuesday, solutions available after one week,
  - No mandatory submission of homeworks
- Weekly quizzes instead
  - Written in the tutorials, duration: 15 minutes
  - Cover the same topics as the last homework
  - Influence your final grading by 30%
  - You need a minimum score of 50%
  - If you present solutions of homework exercises in the tutorial you may cancel up to 4 bad quiz grades

Organization (cont'd)

- Mid-term Exam
  - Tuesday, May 30. Duration: 1 hour
  - Influences your final grading by 20%
- Final Exam
  - Friday, July 21. Duration: 2 hours
  - Influences your final grading by 50%
- Backup Exam
  - Wednesday, October 4
  - If you write the backup exam, your final exam grade is cancelled, i.e., you cannot choose the better one

What this course is (not) about

- CS 578: How to build and use cryptography
- Other security classes:
  - CS 559: (system+network) security
  - CS 650: advanced topics in cryptography
  - CS 300 / CS 600: Several security/crypto (pro-)seminars
- Crypto in use, e.g., SSL:
  - 1. Session-setup: RSA, ElGamal + certificates → shared key
  - 2. Using shared key:
    - Ciphers for privacy
    - MACs for integrity

Is Cryptography only about Encryption?

- PGP: encryption + digital signatures
- User authentication:
  - Password management
  - Smartcards
  - Challenge-response
  - Zero-knowledge authentication
- Wireless: 802.11b WEP
- Other applications:
  - Elections, auctions, copyright protection

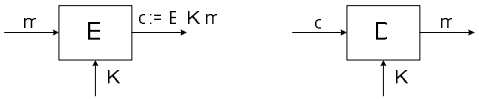
Assumptions on System's Secrecy

- Important to remember from the start: Avoid security by obscurity (!)
  - Worst-case scenario and realistic in nowadays systems
  - Corruption, threads of physical safety, etc.
- Goal:
  - system should be secure even if source code is public
  - Only secret: short key (Kerkhoff's principle)
- Proprietary algorithms = bad algorithms

On (Historical) Ciphers

- History: David Kahn "The Codebreakers"
- Ciphers:

Alice: K Bob: K

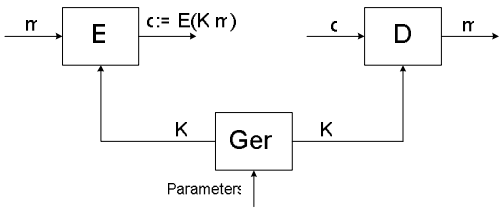


- Symmetric encryption: Both Alice and Bob use the same key K

On (Historical) Ciphers

- Sometimes also key generation explicitly part of the cipher:

Alice: Bob:



Ancient Ciphers: Substitution Cipher

- Oldest cipher in the world, used in the bible, etc.
- Key: K = [a→ f, b → i, c → a, …]
- Encryption of plaintext m = “cbaa” gives ciphertext c = E(K,m) = “aiff”
- #Keys = 26! ≈ 2^{86}

Ancient Ciphers: Caesar’s Cipher

- Used by Caesar in Ancient Rome, 70 B.C.
- Key is fixed table (i.e., actually no cipher): K = [a→ d, b → e, c → f, …] (shift by 3)
- Encryption and decryption as for the substitution cipher

Ancient Ciphers: Shift Cipher

- Generalization of Caesar’s cipher, known usage in history? (Today used in ROT-13)
- Key: K = [a→ g, b → h, c → i, …] (variable shift)
- Encryption and decryption as for the substitution cipher
- #Keys = 26

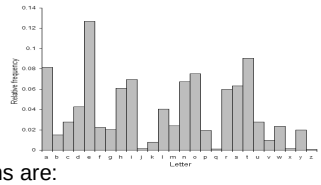
Ancient Ciphers: Substitution Cipher

- Oldest cipher in the world, used in the bible, etc.
- Key: K = [a→ f, b → i, c → a, …]
- Encryption of plaintext m = “cbaa” gives ciphertext c = E(K,m) = “aiff”
- #Keys = 26! ≈ 2^{86}
- Easy to break:
  1. Letter frequency analysis:
     “e” 12.7%, “t” 9.1%, “a” 8.1%
  2. Frequency of pairs of letters
     “th” , “he”, “on”

  → Ciphertext only attack!

Letter Frequencies

- Letter frequencies in average English text.
  Most common:
  - e, t, a, o, i, n
  - s, h, r, d, l, u
  - …



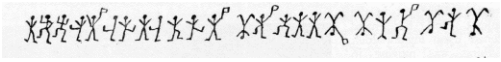
- Common bigrams are:
  - th, he, in, en, nt, re, er, an
- Common trigrams
  - the, and, tha, ent, ing, ion

Examples of Substitution Ciphers

- Edgar Alan Poe, “The Gold Bug”

53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*;:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*;4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

- Sir Arthur Conan Doyle's "Adventure of the Dancing Men"



Examples of Substitution Ciphers

- Edgar Alan Poe, “The Gold Bug”

  A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.

- Sir Arthur Conan Doyle's "Adventure of the Dancing Men"

  ELSIE PREPARE TO MEET THY GOD

Cryptanalysis of Substitution Cipher (1)

```
vxr fezfvtvevtan ytjxrs tf nav fryesr
___ ____________ ______ __ ___ ______
```

Letter frequencies
- v: 5
- r, t, f: 4
- e: 3
- x, a, n, s, y: 2
- j, z: 1

Bigrams
- xr: 2

Guess
vxr=THE

```
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
```


Cryptanalysis of Substitution Cipher (2)

```
vxr fezfvtvevtan ytjxrs tf nav fryesr
THE ____T_T_T___ ___HE_ __ __T _E___E
```

Letter frequencies
-
- t, f: 4
- e: 3
- a, n, s, y: 2
- j, z: 1

Bigrams
- Es, sE: 1

Guess
s=R

```
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
                          E       T   H
```

Saarland University

Cryptanalysis of Substitution Cipher (3)

```
vxr fezfvtvevtan ytjxrs tf nav fryesr
THE ____T_T_T___ ___HER __ __T _E__RE
```

Letter frequencies
-
- t, f: 4
- e: 3
- a, n, y: 2
- j, z: 1

Bigrams

Guess
na=NO

```
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
                              E R     T   H
```

Saarland University

Cryptanalysis of Substitution Cipher (4)

```
vxr fezfvtvevtan ytjxrs tf nav fryesr
THE ____T_T_T_ON ___HER __ NOT _E__RE
```

Letter frequencies
-
- t, f: 4
- e: 3
- y: 2
- j, z: 1

Bigrams

Guess
tf=IS

```
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
O                        N       E R     T   H
```

Saarland University

Cryptanalysis of Substitution Cipher (5)

```
vxr fezfvtvevtan ytjxrs tf nav fryesr
THE S__STIT_TION _I_HER IS NOT SE__RE
```

Letter frequencies
-
-
- e: 3
- y: 2
- j, z: 1

Bigrams

Guess
guess

```
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
O         S              N       E R I   T   H
```

Cryptanalysis of Substitution Cipher (6)

vxr fezfvtvevtan ytjxrs tf nav fryesr
THE SUBSTITUTION CIPHER IS NOT SECURE

Letter frequencies Bigrams Guess

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
O U S P N E R I T H C B

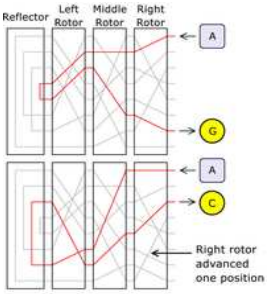
Ancient Ciphers: Vigenere Cipher

- By Vigenere, 1523 - 1570
- Key is randomly chosen string of certain length n.
- Encryption (by means of example)

```
m = THISISBLACKART
K = CRYPTOCRYPTOCR
    --------------
c = VYGHBGDCYRDOTK  (add mod 26)
```

- #Keys = $26^n \approx 2^{4.7n}$
- Easy to break, again frequency analysis

The Enigma machine



Old Ciphers: Rotor Machines

- Roughly 1800 – 1940s.
- Key is initial position of the rotor
- Encryption and decryption by rotations, presumably hard to invert without knowing starting position
- With nowadays knowledge easy to break even by ciphertext only attacks.

The (Semi-)Modern Times

- (1917,1949, One-time Pad)
- 1974: DES (Data Encryption Standard)
- Today: AES (Advanced encryption standard), IDEA, RC5, …

Back to Science: Definition of Ciphers

- Definition (Cipher): A cipher defined over $(\mathcal{K},\mathcal{M},\mathcal{C})$ is a pair of "efficient" algorithms (E,D) where

  E: $\mathcal{K}\times\mathcal{M}\rightarrow\mathcal{C}$ and D: $\mathcal{K}\times\mathcal{C}\rightarrow\mathcal{M}$

  s.t. for all $m\in\mathcal{M}$, $K\in\mathcal{K}$: D(K,E(K,m)) = m.
- Note:
  - E is often randomized,
  - D is always deterministic

The One-time Pad (OTP)

- First “proven secure” cipher: One-time Pad (Vernam 1917, proven in 1949)

  $\mathcal{M} = \mathcal{C} = \{0,1\}^n$, $\mathcal{K} = \{0,1\}^n$

- Secret key K = random bitstring as long as the message
- Encryption: c = E(K,m) = K ⊕ m
- Decryption: m = D(K,c) = K ⊕ c

The One-time Pad (cont’d)

- For OTP being a cipher, we must show: for all $m \in \mathcal{M}$, $K \in \mathcal{K}$, we have D(K,E(K,m)) = m.

  [proof on the board]

- Very fast encryption and decryption
- Problem: Key is as long as the message

Security of Ciphers

- So far only syntactical definition what a cipher is.
- Not addressed yet: What is a secure cipher?

Types of Adversary Success

- Here only for encryption (authentication later in the course)
  1. Total break: find the key
  2. Universal-break: find equivalent method to being able to decrypt with key
  3. Successfully decrypt only selected ciphertexts, but those completely
  4. Successfully learn partial information about single plaintexts (individual bits, checksum, etc.)
- 1. , 2. and 3. clearly unacceptable
- 4. might seem strong, but on the safe side and what else to require?

Security of Ciphers (cont'd)

- So far only syntactical definition what a cipher is.
- Not addressed yet: What is a secure cipher?
- Information theoretic security (Shannon 1949)
- Basic Idea: Define that a ciphertext reveals "no" information about its plaintext

Perfect Secrecy of Ciphers

- Definition (Perfect Secrecy): A cipher (E,D) defined over $(\mathcal{M},\mathcal{K},\mathcal{C})$ has perfect secrecy if for all m_0, $m_1 \in \mathcal{M}$, and for all $c \in \mathcal{C}$:

  $\Pr [c = c';\ K \leftarrow_R \mathcal{K},\ c' \leftarrow E(K,m_0)]$
  $= \Pr [c = c';\ K \leftarrow_R \mathcal{K},\ c' \leftarrow E(K,m_1)]$

- No full introduction of probability notation here
- Suffices to know: We write
  $\Pr [\ E(x_1,\ldots,x_n);\ x_1 \leftarrow A_1(),\ x_2 \leftarrow A_2(x_1),\ldots]$
  to denote probability that E is true after probabilistically generating the x_i's via Alg's A_i

Consequences of Perfect Secrecy

- Perfect Secrecy ensures:
  - Given a ciphertext c, no adversary can tell if the ciphertext contains m_0 or m_1 (for any m_0 and m_1).

→ No ciphertext-only attack possible!
(but other attacks might be possible)

Perfect Secrecy of the OTP

- Lemma: OTP has perfect secrecy.

  [proof on the board]

→ No ciphertext-only attack against the OTP!
(but other attacks might be possible)

Outlook to Next Lecture

- Recall: OTP has perfect secrecy but keys are as long as the message
  → OTP not practical (and as we will see vulnerable to other attacks)
- In the next lecture: How to make the One-time Pad practical
  → stream ciphers