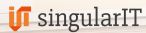


Cryptography

Lecture 1: Introduction & Shift Ciphers

October 16, 2026



Veranstaltung für
MINT-Studierende

Semesterauftakt- Tischtennis

Für Snacks und Getränke ist gesorgt

Jetzt
anmelden!

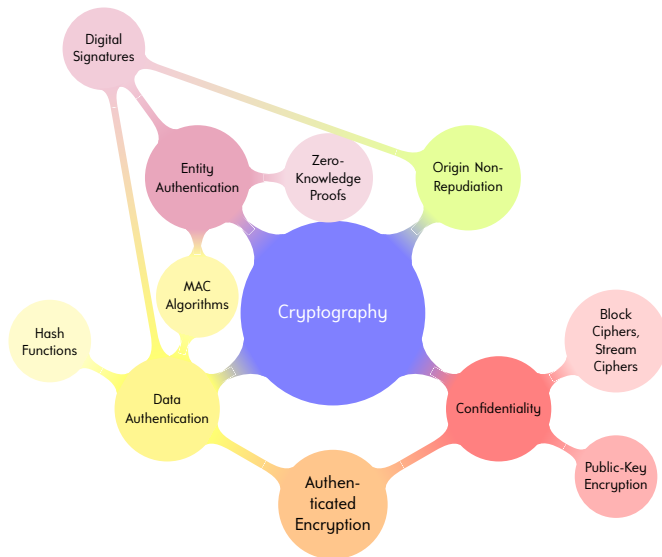


23.10, ab 18 Uhr
Inselstraße 27, 04103 Leipzig

Contents

- 1 Classical cryptography
(Shift & Vigenère cipher, one-time pad, perfect secrecy)
- 2 Security definitions & threat models
(Computational security, CPA & CCA)
- 3 Private-key cryptography
(Message authentication, hash functions, primitives, relevant ciphers)
- 4 Public-key cryptography
(Assumptions, key management, digital signatures, relevant ciphers)

Module Overview



Module Goals

Goals

- Know key notions & cryptographic primitives
- Understand security guarantees
- Able to use cryptography correctly
- Cryptanalysis mindset

Module Goals

Goals

- Know key notions & cryptographic primitives
- Understand security guarantees
- Able to use cryptography correctly
- Cryptanalysis mindset

Non-goals

- Design or implementation of new cryptographic protocols
- Secure zone attacks & defenses (physical security, social engineering)
(→ Course: Foundations of IT security)

- Announcements, lecture slides & exercise sheets

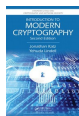
► Moodle

Materials & Literature

- Announcements, lecture slides & exercise sheets

► Moodle

- Recommended literature for self-study & additional detail
(available as hardcopy in library)



Jonathan Katz & Yehuda Lindell

► Introduction to Modern Cryptography

Chapman & Hall, 2014



Bruce Schneier

► Applied Cryptography

Wiley, 2nd edition, 1996



Klaus Schmeh

► Kryptografie — Verfahren, Protokolle, Infrastrukturen

dpunkt.verlag, 6th edition, 2016

Next Dates

LECTURE (FRI 1:15PM)	
Oct 16th	Lecture 1: Introduction & Shift ciphers
23rd	Lecture 2: Vigenère cipher & One-time pad
30th	Lecture 3: Indistinguishability & Limits of Perfect Secrecy
Nov 6th	Lecture 4: Pseudorandom Generators
13th	Lecture 5: Multiple Encryptions
20th	Lecture 6: Pseudorandom Functions
27th	Lecture 7: Operation Modes
Dec 4th	Lecture 8: Message Authentication Codes
11th	Lecture 9: Authenticated Encryption

LECTURE (FRI 1:15PM)	
Dec 18th	Lecture 10: Hash functions
25th	
Jan 1st	
8th	Lecture 11: RSA & Diffie-Hellman assumptions
15th	Lecture 12: Elliptic curves
22nd	Lecture 13: Digital signatures
29th	Lecture 14: Zero-Knowledge Proofs
Feb 5th	Lecture 15: Reserve

- Cancellation of exam registrations up to 11:59pm, January 11, 2027

- Cancellation of exam registrations up to 11:59pm, January 11, 2027

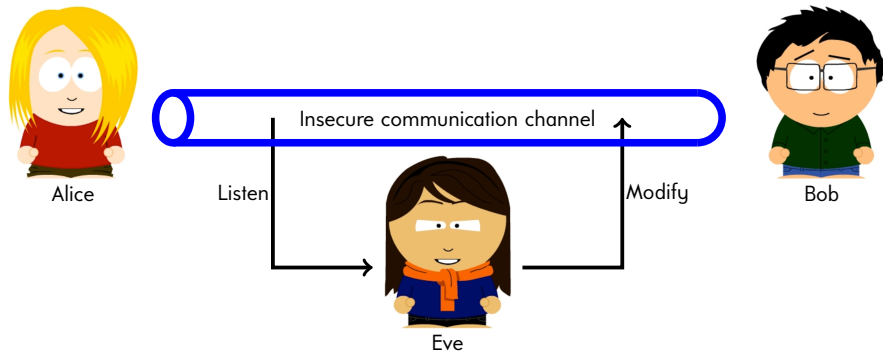
Exam (according to module description)

- Oral 30min
- (change to 'Written 60min' is applied for)

Contents

- 1 **Classical cryptography**
(Shift & Vigenère cipher, one-time pad, perfect secrecy)
- 2 **Security definitions & threat models**
(Computational security, CPA & CCA)
- 3 **Private-key cryptography**
(Message authentication, hash functions, primitives, relevant ciphers)
- 4 **Public-key cryptography**
(Assumptions, key management, digital signatures, relevant ciphers)

Classical Setting



Notes

- Ensure private communication between Alice & Bob
- Shared secret information (key) between Alice & Bob
- Eve only attacks channel
(IT security handles attacks on endpoints)

Some important terms

- **Message** (plaintext) = information to be exchanged

Some important terms

- **Message** (plaintext) = information to be exchanged
- **Ciphertext** = information transmitted on channel

Some important terms

- **Message** (plaintext) = information to be exchanged
- **Ciphertext** = information transmitted on channel
- **Key** = secret information shared by Alice & Bob

Some important terms

- **Message** (plaintext) = information to be exchanged
- **Ciphertext** = information transmitted on channel
- **Key** = secret information shared by Alice & Bob
- **Encryption** = process to derive ciphertext from message

Some important terms

- **Message** (plaintext) = information to be exchanged
- **Ciphertext** = information transmitted on channel
- **Key** = secret information shared by Alice & Bob
- **Encryption** = process to derive ciphertext from message
- **Decryption** = process to derive message from ciphertext

§1.1 Definition (Simplistic encryption scheme)

Simplistic (private-key) encryption scheme for key space K is tuple

$$(\mathcal{M}, \mathcal{C}, \text{enc}, \text{dec})$$

- $\mathcal{M}$ and $\mathcal{C}$ are sets (message & ciphertext space)
- $\text{enc}: K \times \mathcal{M} \rightarrow \mathcal{C}$ and $\text{dec}: K \times \mathcal{C} \rightarrow \mathcal{M}$

§1.1 Definition (Simplistic encryption scheme)

Simplistic (private-key) encryption scheme for key space K is tuple

$$(\mathcal{M}, \mathcal{C}, \text{enc}, \text{dec})$$

- $\mathcal{M}$ and $\mathcal{C}$ are sets (message & ciphertext space)
- $\text{enc}: K \times \mathcal{M} \rightarrow \mathcal{C}$ and $\text{dec}: K \times \mathcal{C} \rightarrow \mathcal{M}$
- $\text{dec}(k, \text{enc}(k, m)) = m$ for all $k \in K$ and $m \in \mathcal{M}$ (correctness)

§1.1 Definition (Simplistic encryption scheme)

Simplistic (private-key) encryption scheme for key space K is tuple

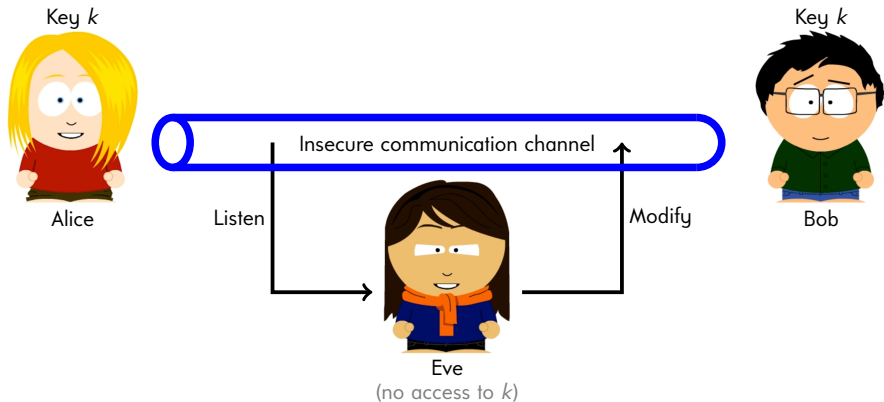
$$(\mathcal{M}, \mathcal{C}, \text{enc}, \text{dec})$$

- $\mathcal{M}$ and $\mathcal{C}$ are sets (message & ciphertext space)
- $\text{enc}: K \times \mathcal{M} \rightarrow \mathcal{C}$ and $\text{dec}: K \times \mathcal{C} \rightarrow \mathcal{M}$
- $\text{dec}(k, \text{enc}(k, m)) = m$ for all $k \in K$ and $m \in \mathcal{M}$ (correctness)

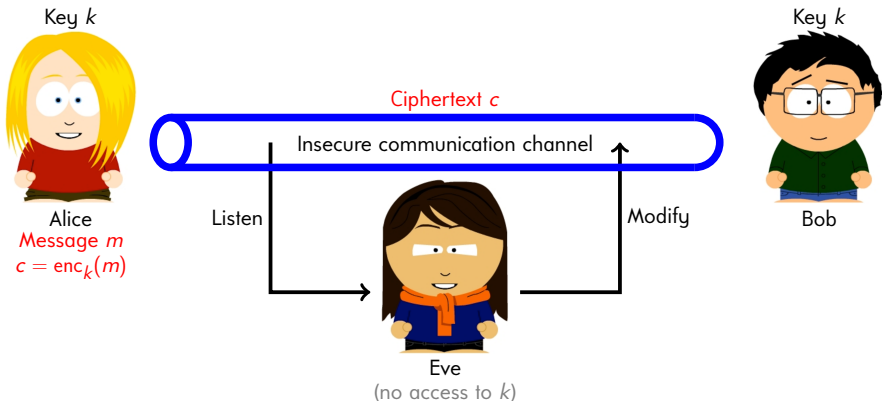
Notes

- We write $\text{enc}_k(m)$ and $\text{dec}_k(c)$ instead of $\text{enc}(k, m)$ and $\text{dec}(k, c)$
- Correctness becomes $\text{dec}_k(\text{enc}_k(m)) = m$

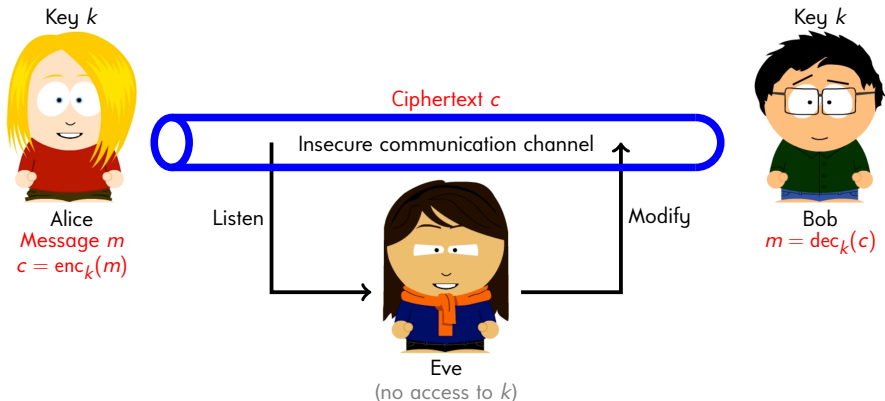
Classical Setting



Classical Setting



Classical Setting



Classical Setting

Notation

- **Alphabet** is simply finite set
- Σ^* is set of all finite sequences of letters from alphabet Σ including empty sequence ε

$$\Sigma^* = \bigcup_{n \in \mathbb{N}} \{\sigma_1 \cdots \sigma_n \mid \sigma_1, \dots, \sigma_n \in \Sigma\}$$

$$\mathbb{N} = \{0, 1, 2, \dots\}$$

Classical Setting

Notation

- **Alphabet** is simply finite set
- Σ^* is set of all finite sequences of letters from alphabet Σ including empty sequence ε

$$\Sigma^* = \bigcup_{n \in \mathbb{N}} \{\sigma_1 \cdots \sigma_n \mid \sigma_1, \dots, \sigma_n \in \Sigma\} \quad \mathbb{N} = \{0, 1, 2, \dots\}$$

- Σ^+ is set of all finite, non-empty sequences of letters from alphabet Σ

$$\Sigma^+ = \bigcup_{n \in \mathbb{N}_+} \{\sigma_1 \cdots \sigma_n \mid \sigma_1, \dots, \sigma_n \in \Sigma\} \quad \mathbb{N}_+ = \{1, 2, 3, \dots\}$$

- Σ^ω is set of all infinite sequences of letters from alphabet Σ

$$\Sigma^\omega = \Sigma^\mathbb{N} = \{f \mid f: \mathbb{N} \rightarrow \Sigma\} = \{\sigma_0 \sigma_1 \sigma_2 \cdots \mid \forall i \in \mathbb{N}: \sigma_i \in \Sigma\}$$

§1.2 Example (Caesar cipher $\approx$ 110 A.D.)

- Key space $K = \{\top\}$ (no key)
- Message space $\mathcal{M} = \Sigma^*$ with $\Sigma = \{0, 1, \dots, 25\}$
(26 letters of Latin alphabet)
- Ciphertext space $\mathcal{C} = \Sigma^*$
- Encryption $\text{enc}_{\top}(m_1, \dots, m_n) = (m_1 + 3 \bmod 26, \dots, m_n + 3 \bmod 26)$
- Decryption $\text{dec}_{\top}(c_1, \dots, c_n) = (c_1 - 3 \bmod 26, \dots, c_n - 3 \bmod 26)$

Caesar Cipher

§1.2 Example (Caesar cipher $\approx$ 110 A.D.)

- Key space $K = \{\top\}$ (no key)
- Message space $\mathcal{M} = \Sigma^*$ with $\Sigma = \{0, 1, \dots, 25\}$
(26 letters of Latin alphabet)
- Ciphertext space $\mathcal{C} = \Sigma^*$
- Encryption $\text{enc}_{\top}(m_1, \dots, m_n) = (m_1 + 3 \bmod 26, \dots, m_n + 3 \bmod 26)$
- Decryption $\text{dec}_{\top}(c_1, \dots, c_n) = (c_1 - 3 \bmod 26, \dots, c_n - 3 \bmod 26)$

Illustration

- “hello” $\rightsquigarrow$ encoded as $m = (7, 4, 11, 11, 14)$
- Ciphertext $c = (10, 7, 14, 14, 17) = \text{enc}_{\top}(7, 4, 11, 11, 14)$
which represents “khood”
- Message $m = (7, 4, 11, 11, 14) = \text{dec}_{\top}(10, 7, 14, 14, 17) = \text{dec}_{\top}(c)$
which represents “hello”

Caesar Cipher

Illustration

message		h	e	l	l	o
---------	--	---	---	---	---	---

Caesar Cipher

Illustration

message		h	e	l	l	o
+1		i	f	m	m	p

Caesar Cipher

Illustration

message	h	e	l	l	o
+1	i	f	m	m	p
+2	j	g	n	n	q

Caesar Cipher

Illustration

message	h	e	l	l	o
+1	i	f	m	m	p
+2	j	g	n	n	q
+3	k	h	o	o	r

Kerckhoffs' Principle

§1.3 Principle (Kerckhoffs 1883)

Encryption scheme is **not secret**; only the key is.

Notes

- Rediscovered by Claude Shannon (1949): *Shannon's maxim*
- Opposite: **Security through obscurity**

Auguste Kerckhoffs (* 1835; † 1903)

- Dutch linguist & cryptographer
- Professor of German in Paris
- Director of the Academy of Volapük



Kerckhoffs' Principle

Kerckhoffs' design principles (for military ciphers)

- ❶ Practically, if not mathematically, indecipherable

Kerckhoffs' Principle

Kerckhoffs' design principles (for military ciphers)

- ① Practically, if not mathematically, indecipherable
- ② **No secrecy required** (unproblematic even if system known to enemy)

Kerckhoffs' Principle

Kerckhoffs' design principles (for military ciphers)

- ① Practically, if not mathematically, indecipherable
- ② **No secrecy required** (unproblematic even if system known to enemy)
- ③ Key can be communicated & remembered without notes & changed or modified at will

Kerckhoffs' Principle

Kerckhoffs' design principles (for military ciphers)

- ① Practically, if not mathematically, indecipherable
- ② **No secrecy required** (unproblematic even if system known to enemy)
- ③ Key can be communicated & remembered without notes & changed or modified at will
- ④ Applicable to telegraph communication

Kerckhoffs' Principle

Kerckhoffs' design principles (for military ciphers)

- 1 Practically, if not mathematically, indecipherable
- 2 **No secrecy required** (unproblematic even if system known to enemy)
- 3 Key can be communicated & remembered without notes & changed or modified at will
- 4 Applicable to telegraph communication
- 5 Portable & operable by single person

Kerckhoffs' Principle

Kerckhoffs' design principles (for military ciphers)

- ① Practically, if not mathematically, indecipherable
- ② **No secrecy required** (unproblematic even if system known to enemy)
- ③ Key can be communicated & remembered without notes & changed or modified at will
- ④ Applicable to telegraph communication
- ⑤ Portable & operable by single person
- ⑥ Easy to use even under duress (no long lists of memorized rules)

§1.4 Example (Shift cipher)

- Key space $K = \{0, \dots, 25\}$
- Message space $\mathcal{M} = \Sigma^*$ with $\Sigma = \{0, 1, \dots, 25\}$
(26 letters of Latin alphabet)
- Ciphertext space $\mathcal{C} = \Sigma^*$
- Encryption $\text{enc}_k(m_1, \dots, m_n) = (m_1 + k \bmod 26, \dots, m_n + k \bmod 26)$
- Decryption $\text{dec}_k(c_1, \dots, c_n) = (c_1 - k \bmod 26, \dots, c_n - k \bmod 26)$

§1.4 Example (Shift cipher)

- Key space $K = \{0, \dots, 25\}$
- Message space $\mathcal{M} = \Sigma^*$ with $\Sigma = \{0, 1, \dots, 25\}$
(26 letters of Latin alphabet)
- Ciphertext space $\mathcal{C} = \Sigma^*$
- Encryption $\text{enc}_k(m_1, \dots, m_n) = (m_1 + k \bmod 26, \dots, m_n + k \bmod 26)$
- Decryption $\text{dec}_k(c_1, \dots, c_n) = (c_1 - k \bmod 26, \dots, c_n - k \bmod 26)$

Illustration

- “hello” $\rightsquigarrow$ encoded as $m = (7, 4, 11, 11, 14)$
- Ciphertext $c = (20, 17, 24, 24, 1) = \text{enc}_{13}(7, 4, 11, 11, 14)$
which represents “uryyb”
- Message $m = (7, 4, 11, 11, 14) = \text{dec}_{13}(20, 17, 24, 24, 1) = \text{dec}_{13}(c)$
which represents “hello”

Shift Cipher

Cryptanalysis of shift cipher

Decrypt: “**vd****kkcnmd**” (21, 3, 10, 10, 2, 13, 12, 3)

Shift Cipher

Cryptanalysis of shift cipher

Decrypt: “**vdkkcnmd**” (21, 3, 10, 10, 2, 13, 12, 3)

Brute-force (exhaustive search) attack

(try every possible key)

$\text{dec}_0(c) = \text{vdkkcnmd}$	$\text{dec}_1(c) = \text{ucjjbmlc}$	$\text{dec}_2(c) = \text{tbiialkb}$
$\text{dec}_3(c) = \text{sahhzhkja}$	$\text{dec}_4(c) = \text{rzggyjiz}$	$\text{dec}_5(c) = \text{qyffxiyh}$
$\text{dec}_6(c) = \text{pxeewhgx}$	$\text{dec}_7(c) = \text{owddvgfw}$	$\text{dec}_8(c) = \text{nvccufev}$
$\text{dec}_9(c) = \text{mubbtdu}$	$\text{dec}_{10}(c) = \text{ltaasdct}$	$\text{dec}_{11}(c) = \text{kszzrcbs}$
$\text{dec}_{12}(c) = \text{jryyqbar}$	$\text{dec}_{13}(c) = \text{iqxxpazq}$	$\text{dec}_{14}(c) = \text{hpwwozyp}$
$\text{dec}_{15}(c) = \text{govvnyxo}$	$\text{dec}_{16}(c) = \text{fnumxwn}$	$\text{dec}_{17}(c) = \text{emttlwvm}$
$\text{dec}_{18}(c) = \text{dlsskvul}$	$\text{dec}_{19}(c) = \text{ckrrjutk}$	$\text{dec}_{20}(c) = \text{bjqqitsj}$
$\text{dec}_{21}(c) = \text{aipphsri}$	$\text{dec}_{22}(c) = \text{zhoogrqh}$	$\text{dec}_{23}(c) = \text{ygnnfqpg}$
$\text{dec}_{24}(c) = \text{xfmepof}$	$\text{dec}_{25}(c) = \text{welldone}$	

Silent assumptions

- English plaintext
- Sufficiently long ciphertext for single valid plaintext

§1.5 Principle (Sufficient key space)

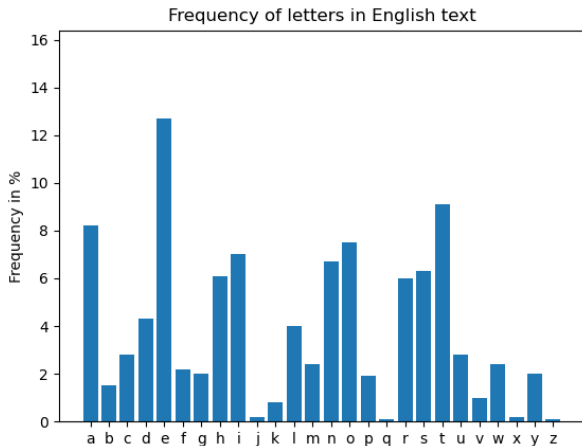
Key space must be sufficiently large

(more precise later)

Shift Cipher

Better cryptanalysis of shift cipher

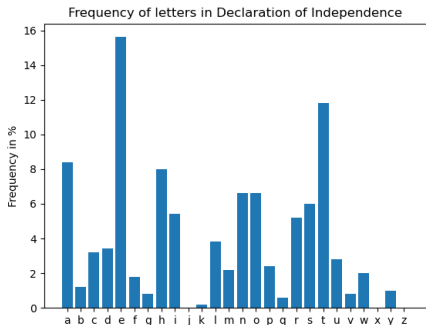
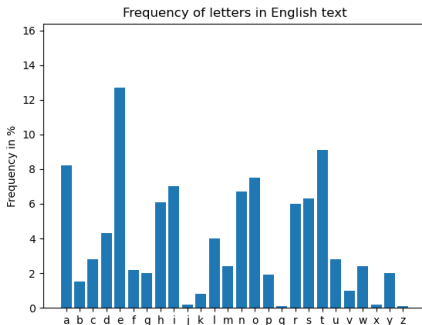
- Utilize English language specifics (letter frequencies, common doubles)
- Determine invariants



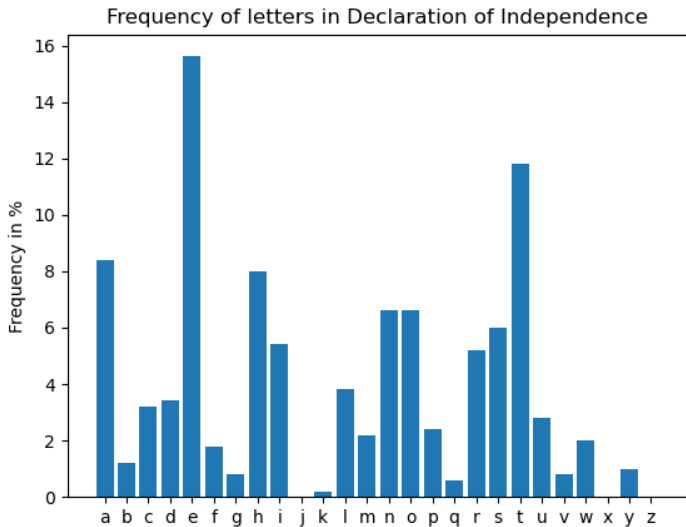
Shift Cipher

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 of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation.

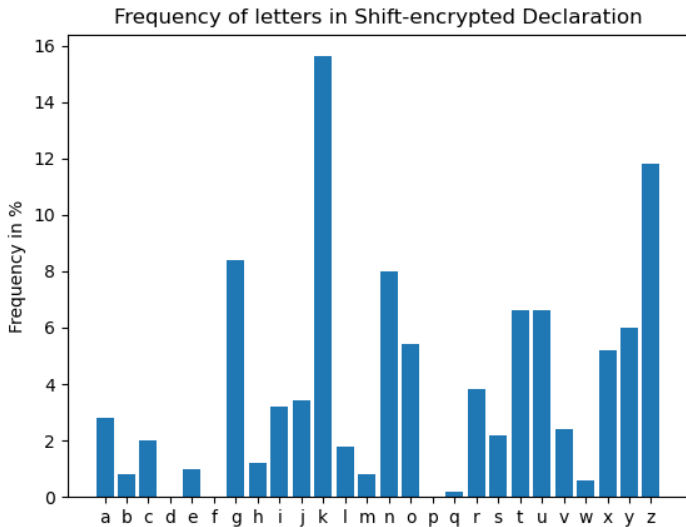
We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. — [US Declaration of Independence](#)



Shift Cipher



Shift Cipher



Attack

- Letter counts b_i^m on sufficiently long message m with $n = |m|$

$$I(m) = 26 \sum_{i=0}^{25} \frac{b_i^m(b_i^m-1)}{n(n-1)} \approx 26 \sum_{i=0}^{25} p_i^2 = 1.706926 = I$$

Shift Cipher

Attack

- Letter counts b_i^m on sufficiently long message m with $n = |m|$
$$I(m) = 26 \sum_{i=0}^{25} \frac{b_i^m(b_i^m-1)}{n(n-1)} \approx 26 \sum_{i=0}^{25} p_i^2 = 1.706926 = I$$
- Letter frequencies $f_i(c)$ on sufficiently long ciphertext c with shift k
$$I_k(c) = 26 \sum_{i=0}^{25} f_{(i+k \bmod 26)}(c)p_i = 26 \sum_{i=0}^{25} f_i(m)p_i \approx I$$

Shift Cipher

Attack

- Letter counts b_i^m on sufficiently long message m with $n = |m|$
$$I(m) = 26 \sum_{i=0}^{25} \frac{b_i^m(b_i^m-1)}{n(n-1)} \approx 26 \sum_{i=0}^{25} p_i^2 = 1.706926 = I$$
- Letter frequencies $f_i(c)$ on sufficiently long ciphertext c with shift k
$$l_k(c) = 26 \sum_{i=0}^{25} f_{(i+k \bmod 26)}(c)p_i = 26 \sum_{i=0}^{25} f_i(m)p_i \approx I$$

$$l_0(c) = 0.75075$$

$$l_1(c) = 0.54275$$

$$l_2(c) = 1.27075$$

$$l_3(c) = 1.17000$$

$$l_4(c) = 0.63050$$

$$l_5(c) = 0.70850$$

$$l_6(c) = 1.24150$$

$$l_7(c) = 0.84825$$

$$l_8(c) = 1.04000$$

$$l_9(c) = 1.20575$$

$$l_{10}(c) = 1.69000$$

$$l_{11}(c) = 0.77675$$

$$l_{12}(c) = 0.84500$$

$$l_{13}(c) = 0.57850$$

$$l_{14}(c) = 0.78975$$

$$l_{15}(c) = 0.90675$$

$$l_{16}(c) = 0.85150$$

$$l_{17}(c) = 1.40075$$

$$l_{18}(c) = 0.95875$$

$$l_{19}(c) = 0.92625$$

$$l_{20}(c) = 0.79625$$

$$l_{21}(c) = 1.43000$$

$$l_{22}(c) = 1.15050$$

$$l_{23}(c) = 0.76700$$

$$l_{24}(c) = 1.02375$$

$$l_{25}(c) = 1.76475$$

Extra material

- Derive formulas used in better cryptanalysis (aka. coincidence counting)
 - ▶ Start with Pearson's χ^2 statistic
 - ▶ Make one of the distributions uniform
 - ▶ Interpret I and $I(c)$ as “similarity to uniform distribution”
- Develop method to detect shift cipher

Cryptanalysis of Shift Cipher

Pearson's χ^2 statistic

(used to compare categorical distributions)

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i}$$

Cryptanalysis of Shift Cipher

Pearson's χ^2 statistic

(used to compare categorical distributions)

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i}$$

Simplify

$$\begin{aligned}\chi^2(p., q.) &= \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i} = \sum_{i=0}^{25} \frac{p_i^2 - 2p_i q_i + q_i^2}{q_i} \\&= \sum_{i=0}^{25} \left(\frac{p_i^2}{q_i} - 2p_i + q_i \right) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 2 \underbrace{\sum_{i=0}^{25} p_i}_{=-2} + \underbrace{\sum_{i=0}^{25} q_i}_{=1} \\&= \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1\end{aligned}$$

Cryptanalysis of Shift Cipher

Pearson's χ^2 statistic

(used to compare categorical distributions)

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i}$$

Simplify

$$\begin{aligned}\chi^2(p., q.) &= \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i} = \sum_{i=0}^{25} \frac{p_i^2 - 2p_iq_i + q_i^2}{q_i} \\ &= \sum_{i=0}^{25} \left(\frac{p_i^2}{q_i} - 2p_i + q_i \right) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 2 \underbrace{\sum_{i=0}^{25} p_i}_{=-2} + \underbrace{\sum_{i=0}^{25} q_i}_{=1} \\ &= \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1\end{aligned}$$

Cryptanalysis of Shift Cipher

Pearson's χ^2 statistic

(used to compare categorical distributions)

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i}$$

Simplify

$$\begin{aligned}\chi^2(p., q.) &= \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i} = \sum_{i=0}^{25} \frac{p_i^2 - 2p_iq_i + q_i^2}{q_i} \\&= \sum_{i=0}^{25} \left(\frac{p_i^2}{q_i} - 2p_i + q_i \right) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 2 \underbrace{\sum_{i=0}^{25} p_i}_{=-2} + \underbrace{\sum_{i=0}^{25} q_i}_{=1} \\&= \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1\end{aligned}$$

Cryptanalysis of Shift Cipher

Pearson's χ^2 statistic

(used to compare categorical distributions)

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i}$$

Simplify

$$\begin{aligned}\chi^2(p., q.) &= \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i} = \sum_{i=0}^{25} \frac{p_i^2 - 2p_i q_i + q_i^2}{q_i} \\&= \sum_{i=0}^{25} \left(\frac{p_i^2}{q_i} - 2p_i + q_i \right) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - \underbrace{2 \sum_{i=0}^{25} p_i}_{=-2} + \underbrace{\sum_{i=0}^{25} q_i}_{=1} \\&= \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1\end{aligned}$$

Cryptanalysis of Shift Cipher

Pearson's χ^2 statistic

(used to compare categorical distributions)

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i}$$

Simplify

$$\begin{aligned}\chi^2(p., q.) &= \sum_{i=0}^{25} \frac{(p_i - q_i)^2}{q_i} = \sum_{i=0}^{25} \frac{p_i^2 - 2p_i q_i + q_i^2}{q_i} \\&= \sum_{i=0}^{25} \left(\frac{p_i^2}{q_i} - 2p_i + q_i \right) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - \underbrace{2 \sum_{i=0}^{25} p_i}_{=-2} + \underbrace{\sum_{i=0}^{25} q_i}_{=1} \\&= \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1\end{aligned}$$

Cryptanalysis of Shift Cipher

Simplified Pearson's χ^2 statistic

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1$$

Cryptanalysis of Shift Cipher

Simplified Pearson's χ^2 statistic

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1$$

Fix distribution $q.$ to uniform & take English letter distribution $p.$

(compare English distribution $p.$ to uniform distribution)

$$d(p.) = \chi^2(p., q.) = \sum_{i=0}^{25} \frac{p_i^2}{26^{-1}} - 1 = 26 \sum_{i=0}^{25} p_i^2 - 1 = 0.706926$$

Cryptanalysis of Shift Cipher

Simplified Pearson's χ^2 statistic

$$\chi^2(p., q.) = \sum_{i=0}^{25} \frac{p_i^2}{q_i} - 1$$

Fix distribution $q.$ to uniform & take English letter distribution $p.$

(compare English distribution $p.$ to uniform distribution)

$$d(p.) = \chi^2(p., q.) = \sum_{i=0}^{25} \frac{p_i^2}{26^{-1}} - 1 = 26 \sum_{i=0}^{25} p_i^2 - 1 = 0.706926$$

We instead used *expected index of coincidence*

(simply without '-1')

$$I = 26 \sum_{i=0}^{25} p_i^2 = 1.706926$$

Cryptanalysis of Shift Cipher

Index of coincidence for counts b_i^c with $n = |c|$

(26 times probability that 2 random locations in c carry same letter)

$$I(c) = 26 \sum_{i=0}^{25} \frac{b_i^c(b_i^c - 1)}{n(n-1)}$$

Cryptanalysis of Shift Cipher

Index of coincidence for counts b_i^c with $n = |c|$

(26 times probability that 2 random locations in c carry same letter)

$$I(c) = 26 \sum_{i=0}^{25} \frac{b_i^c(b_i^c - 1)}{n(n-1)}$$

Invariant for all shift-encryptions of m

$$I(m) = I(\text{enc}_k(m)) = I(c) = 1.857143 \approx 1.706926 = I \quad \text{for all } k$$

Cryptanalysis of Shift Cipher

Index of coincidence for counts b_i^c with $n = |c|$

(26 times probability that 2 random locations in c carry same letter)

$$I(c) = 26 \sum_{i=0}^{25} \frac{b_i^c(b_i^c - 1)}{n(n-1)}$$

Invariant for all shift-encryptions of m

$$I(m) = I(\text{enc}_k(m)) = I(c) = 1.857143 \approx 1.706926 = I \quad \text{for all } k$$

(Somewhat) language-specific

Language	I
English	1.7
German	2.1
Spanish	1.9

(can be used to check for shift ciphers & for particular languages)

Cryptanalysis of Shift Cipher

Compare all shifted distributions to reference English p .

$$\chi_k^2(c, p.) = \sum_{i=0}^{25} \frac{f_{i+k \bmod 26}(c)^2}{p_i} - 1$$

$\chi_0^2(c, p.) = 11.27$	$\chi_1^2(c, p.) = 35.12$	$\chi_2^2(c, p.) = 6.77$
$\chi_3^2(c, p.) = 26.43$	$\chi_4^2(c, p.) = 73.70$	$\chi_5^2(c, p.) = 28.88$
$\chi_6^2(c, p.) = 33.25$	$\chi_7^2(c, p.) = 6.32$	$\chi_8^2(c, p.) = 9.11$
$\chi_9^2(c, p.) = 6.71$	$\chi_{10}^2(c, p.) = 2.01$	$\chi_{11}^2(c, p.) = 66.31$
$\chi_{12}^2(c, p.) = 27.84$	$\chi_{13}^2(c, p.) = 109.61$	$\chi_{14}^2(c, p.) = 21.76$
$\chi_{15}^2(c, p.) = 15.69$	$\chi_{16}^2(c, p.) = 11.99$	$\chi_{17}^2(c, p.) = 5.02$
$\chi_{18}^2(c, p.) = 5.99$	$\chi_{19}^2(c, p.) = 16.95$	$\chi_{20}^2(c, p.) = 94.43$
$\chi_{21}^2(c, p.) = 4.14$	$\chi_{22}^2(c, p.) = 33.15$	$\chi_{23}^2(c, p.) = 21.00$
$\chi_{24}^2(c, p.) = 13.41$	$\chi_{25}^2(c, p.) = 2.51$	

Exercises

- 1 Show $\lim_{|m| \rightarrow \infty} I(m) = I$ for all English messages m (i.e. $p_i = \frac{b_i^m}{|m|}$)
(i.e. I is indeed the expected index of coincidence)
- 2 Why should $\chi_k^2(c, p.)$ be low?
(What is its optimal value?)

Summary

- Basic notions
- Classic encryption setting
- Caesar cipher
- Shift cipher
- Cryptanalysis of shift cipher