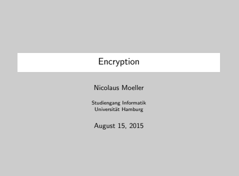
Encryption

Nicolaus Moeller

Studiengang Informatik
Universität Hamburg

August 15, 2015



Encryption

Nicolaus Moeller

Studiengang Informatik
Universität Hamburg

August 15, 2015

First of all, what is encryption? According to Wikipedia: ”Encryption is the process of encoding a message such that only authorized parties can read it.” [23] Encryption doesn’t mean that non-authorized parties can not intercept the message: It only means that the content is inaccesible to them. We’re going to see some of the first cryptographic-techniques used in history that will help us gain an understanding of the subject. This presentation was meant as a small introduction to cryptography, to show how and why is encryption actually possible with some examples of encryption software and hardware at the end.

Contents

1 Introduction

2 Cryptography

3 Modern examples

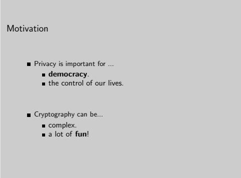
4 Summary

5 Bibliography

Motivation

- Privacy is important for ...
  - **democracy**.
  - the control of our lives.

- Cryptography can be...
  - complex.
  - a lot of **fun**!



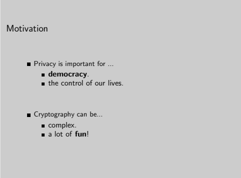
Motivation

- Privacy is important for ...
  - **democracy**.
  - the control of our lives.
- Cryptography can be...
  - complex.
  - a lot of **fun**!

There are a lot of reasons for why you should care about encryption today. In this slide you'll see a non-exhaustive list about the importance of encryption today.

Privacy, and thats what we can achieve with proper encryption, is important for democracy. Some governments, intelligence agencies and other entities around the world gather information of its fellow citizens for political or economic reasons. Today we're creating when we use our phones, our computers, or the internet, a vast amount of information, information that speaks about us. If someone knows something about ourselves that could hurt our reputation we could become a target of blackmail or extorsion. We want to be able to protect ourselves, and it's our right also to do so.

In other words: information is power, and encryption keeps power balanced. Hence, the importance of encryption for democracy has become evident.



Motivation

- Privacy is important for ...
  - **democracy**.
  - the control of our lives.
- Cryptography can be...
  - complex.
  - a lot of **fun**!

Mathematics, particularly number theory, plays a very important part in Encryption and cryptography : It gets complex and difficult very fast. Nevertheless, another source of motivation for studying encryption is that it is actually a lot of fun.

Problem

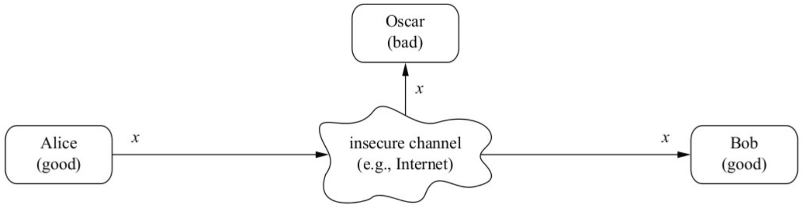


Figure : [29, p.5]

Problem

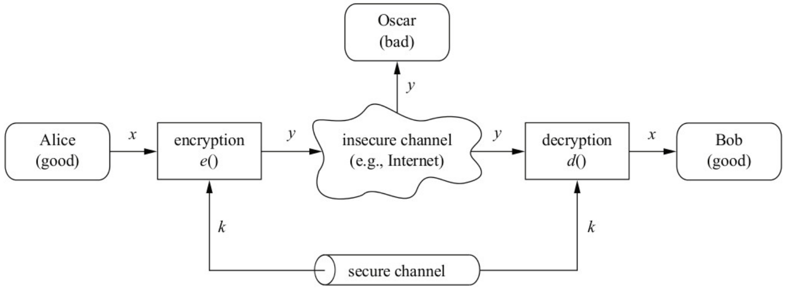
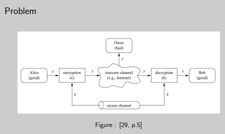


Figure : [29, p.5]



We have Alice and Bob, and they want to communicate freely though an insecure channel without Oscar listening. The insecure channel is for our purpose uninteresting: It could be the internet, pencil and paper, or any other way of transmitting a message. We will allways assume that we have eavesdroppers. The solution: Encrypting the data x with some key k, meaning transforming the data x in such a format that it's not possible to extract the contents of the message except for authorized parties, who will be able to reverse the transformation (decryption) from y to x with the same key k, which was used to encrypt.
We are going to focus mostly on the special case where we just have Alice encrypting, for example her harddisk, for her to decrypt sometime later in the future. In this case, Alice wouldn't have to worry about sending the key to someone, because she's the one doing the decryption.
(Important: Do not confuse encryption with encoding or hashing.)

Cryptology

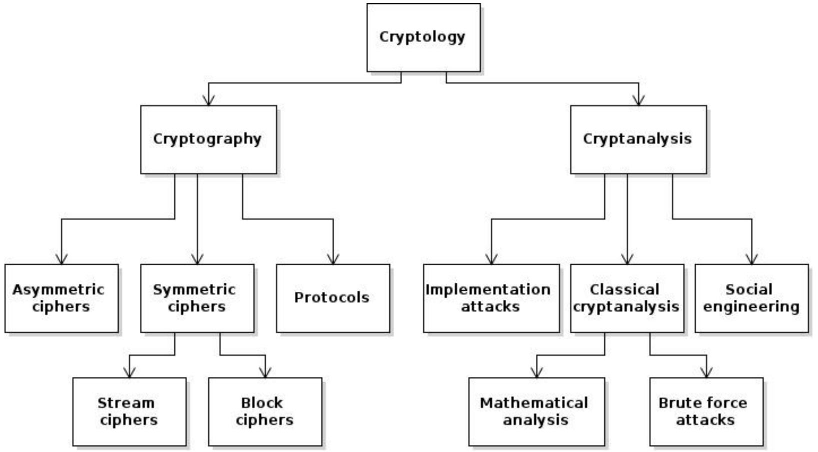
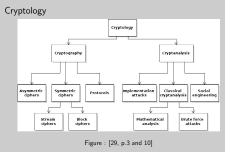
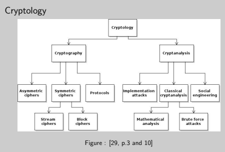


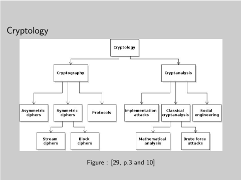
Figure : [29, p.3 and 10]



This Graph was faithfully constructed from the book: Understanding Cryptography. [29]
Cryptology is the scientific study of hidden messages. And it can be divided into to further subfields. That is, the field of cryptography and the field of cryptoanalysis. Cryptography deals with the creation and planning of techniques and systems that try to prevent certain people from being able to read a message (that is possibly being transmitted). Cryptoanalysis is the science of breaking those systems. Some people will call it more an art than a science (a lot of creativity is involved in breaking cryptographic constructions).



In Cryptography we have different types of systems that we can build. One not included in the digram, is the science of steganography which is the science of transmitting a message without the eavesdropper even knowing that a message is being send. We're not going to look at asymmetric ciphers (also called public ciphers). We saw on the first semester of our career the mathematical basics of an RSA-cipher (a well known public cipher), which exploits the fact, that its easier to exponentiate a number than it is to factorize it. We're not going to see protocols either. The mayority of cryptographic applications are hybrid shemes, that means they use a mix of these ciphers to ensure a secure system. Symmetric ciphers are cryptosystems in which there is only one key, known by Alice and Bob. We're going to deal with streamciphers and blockciphers. Streamciphers are cryptosystems that encrypt information bit by bit, while blockciphers encrypt a sequence of bits at a time.



Cryptology

Figure : [29, p.3 and 10]

In Cryptanalysis, we have Implementation attacks, which are only useful when you have physical access to the hardware that is implementing the encryption. Maybe you could count the seconds that the encryption takes, and obtain useful information about that. These are rather complicated and not to be explored on this presentation. The same counts for social engineering attacks (coercing, stealing, espionage, extorsion). We're going to focus more on the classical attacks: mathematical analysis and brute force attacks.

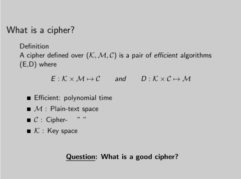
What is a cipher?

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

$$E : \mathcal{K} \times \mathcal{M} \mapsto \mathcal{C} \qquad \textit{and} \qquad D : \mathcal{K} \times \mathcal{C} \mapsto \mathcal{M}$$

- Efficient: polynomial time
- $\mathcal{M}$: Plain-text space
- $\mathcal{C}$: Cipher- " "
- $\mathcal{K}$: Key space

Question: What is a good cipher?



What is a cipher?
Definition
A cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ is a pair of *efficient* algorithms (E,D) where
$E : \mathcal{K} \times \mathcal{M} \mapsto \mathcal{C}$ *and* $D : \mathcal{K} \times \mathcal{C} \mapsto \mathcal{M}$
- Efficient: polynomial time
- $\mathcal{M}$: Plain-text space
- $\mathcal{C}$: Cipher- " "
- $\mathcal{K}$: Key space
Question: What is a good cipher?

Definitions:
A cipher are two algorithms: One performs the encryption, the other one decryption.
About the mathematical definition on the slide [27]:

- Both Algorithms must run efficiently, for the cipher to be of practical use.
- Key-space: Could be seen as the set of all the possible keys (or a list of possible passwords if you like) that could potentially be used to encrypt a message.
- Plaintext-space: Set of all possible messages that can be decrypted.
- Ciphertext-space: Set of all encrypted messages that could have been produced given a plaintext and a key.

The first question that we should ask ourselves: What is a good cipher?

Substitution cipher

- Substitute character of the alphabet for another character.
- A particular example: Caesar cipher

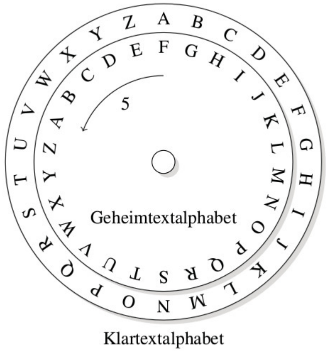
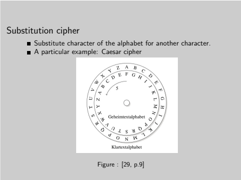


Figure : [29, p.9]

2015-08-15

Encryption
└─Cryptography
└─Cryptosystems
└─Substitution cipher


Substitution cipher

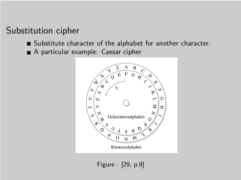
- Substitute character of the alphabet for another character.
- A particular example: Caesar cipher

Figure : [29, p.9]

To answer that question, we will look at the first ciphers used in history. The first type of cipher that we will see is the substitution cipher, where you replace every symbol of the plaintext to another symbol. One particular type was used by Caesar to communicate with his generals: A shift cipher. [29, p.18] In this type of cipher you replace each letter of the plaintext to another letter, according to a number and the order of the alphabet. For example: if the chosen key is the number 5, you'll have to replace every letter of the plaintext as such: 'A' with 'F', 'B' with 'G', and so on (See figure).

2015-08-15

Encryption
└─Cryptography
└─Cryptosystems
└─Substitution cipher


Substitution cipher

- Substitute character of the alphabet for another character.
- A particular example: Caesar cipher

Figure : [29, p.9]

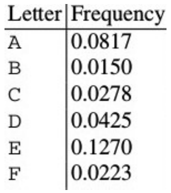
The shift-cipher has a key-space that contains 26 possible keys, namely the numbers 0 to 25. For Caesars enemies to decrypt a message they would have only needed to decrypt a portion of the intercepted message with 25 different keys to see if something meaningful comes out. This illustrates how important the size of the key-space actually is.
Why would Caesar use such an easy to break, primitive cipher? The strength of a cipher will depend mostly of the time it was created. In the time of Caesar (and for the purpose it was used) a stronger cipher wasn't needed.

As the centuries went by and cryptoanalysis began to become more and more a serious endeavour, stronger ciphers were needed.

Encryption
└─Cryptography
└─Cryptosystems

Substitution cipher cont.

- Brute force attack: $|\mathcal{K}| = 26! \approx 2^{88}$
- Letter frequency attack:



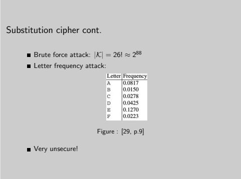
Letter	Frequency
A	0.0817
B	0.0150
C	0.0278
D	0.0425
E	0.1270
F	0.0223

Figure : [29, p.9]

- Very unsecure!

2015-08-15

Encryption
└─Cryptography
└─Cryptosystems
└─Substitution cipher cont.


Substitution cipher cont.

- Brute force attack: $|\mathcal{K}| = 26! \approx 2^{88}$
- Letter frequency attack:

Letter	Frequency
A	0.0817
B	0.0150
C	0.0278
D	0.0425
E	0.1270
F	0.0223

Figure : [29, p.9]

- Very unsecure!

Let's now see the generic substitution cipher, where we replace each letter of the alphabet for another letter (without taking into account the order of the alphabet): In this case the size of the key-space is 26!.
Trying every possible key would take a lot of time. Is this cipher secure?
Answer: No! Mayor weakness: Each plaintext symbol maps to the same ciphertext symbol. The statistical properties of the plain text are preserved in the ciphertext. It so happens that languages use some letters more frequently than others. With a so called letter-frequency attack, this cipher is easily broken.

Vigenere cipher

A	0
B	1
C	2
...	...

- Encrypt using modular arithmetic

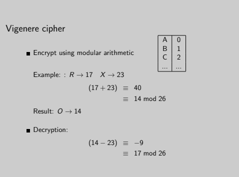
  Example: : $R \to 17 \quad X \to 23$

$$\begin{aligned}(17+23) &\equiv 40\\ &\equiv 14 \bmod 26\end{aligned}$$

  Result: $O \to 14$

- Decryption:

$$\begin{aligned}(14-23) &\equiv -9\\ &\equiv 17 \bmod 26\end{aligned}$$



Vigenere cipher
Encrypt using modular arithmetic
Example: : $R \to 17 \quad X \to 23$ $(17+23) \equiv 40 \equiv 14 \bmod 26$
Result: $O \to 14$
Decryption: $(14-23) \equiv -9 \equiv 17 \bmod 26$

The next cipher we'll see is the Vigenère cipher published in 1585 by the french translator and diplomat Blaise de Vigenère. It was considered unbreakable for a relatively long time. It uses a series of (preferably different) Caesar ciphers.
Before we see an example of the Vigenère cipher, we should see a short review of algebra and modular arithmetic that will help us understand how the Vigenère cipher works (See slide and [29, p.13]).

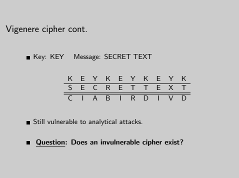
Vigenere cipher cont.

- Key: KEY Message: SECRET TEXT

K	E	Y	K	E	Y	K	E	Y	K
S	E	C	R	E	T	T	E	X	T
C	I	A	B	I	R	D	I	V	D

- Still vulnerable to analytical attacks.

- **<u>Question</u>: Does an invulnerable cipher exist?**



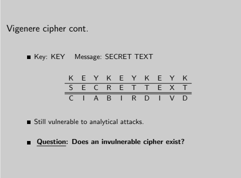
Vigenere cipher cont.
Key: KEY Message: SECRET TEXT
K E Y K E Y K E Y K
S E C R E T T E X T
C I A B I R D I V D
Still vulnerable to analytical attacks.
Question: Does an invulnerable cipher exist?

We want to encrypt the message "SECRET TEXT" and we choose the key "KEY".
In this cipher we use the caesar cipher on every letter of the plaintext according to the key. In this example: 'S' will be shifted 10 positions down the alphabet because 'K', the first letter of the key, is the 10th letter of the alphabet. The next letter 'E' will be shifted 4 positions down the alphabet because 'E', the second letter of the key, maps to 4. And so on. [32] Notice:

- CIA BIRD: This is the actual encryption! [25] We see patterns or meaning in randomness that may not be there.
- The T is encrypted twice as an R and the next time as a D. (Good)
- Unfortunately: All our E's are encrypted in the same way. This came about because we used an english word as a key (and 'E' is a very frequent letter in the english language) and secondly we chosed a very short key.

2015-08-15

Encryption
└Cryptography
└Cryptosystems
└Vigenere cipher cont.



Vigenere cipher cont.

- Key: KEY Message: SECRET TEXT

K	E	Y	K	E	Y	K	E	Y	K
S	E	C	R	E	T	T	E	X	T
C	I	A	B	I	R	D	I	V	D

- Still vulnerable to analytical attacks.
- **Question: Does an invulnerable cipher exist?**

We clearly see that this cipher is stronger than the Caesar cipher because it potentially hides the statistical properties of the plaintext (in the example: 'T' is encrypted twice as an 'R' and a 'D'). We can already see that the strength of this cipher will depend of the length of the key: The size of the key space is 26 to the power of n, where n is the length of the key.

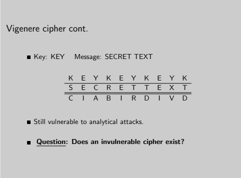
Let's assume for a moment that the key is much shorter than the message. In this case the key is repeated every number of times. If we could guess the length of the key the message could be broken, because its just a series of caesar ciphers which we know how to break: We would use a letter-frequency analysis on those letter that were encrypted with the same letter of the key. The only problem would be to determine the key length (for more information about that see: Kasiski examination and Friedman test).

Although a much better cipher than the previous one, it is still breakable.

What properties should an unbreakable cipher have, if such exist?

2015-08-15

Encryption
└Cryptography
└Cryptosystems
└Vigenere cipher cont.



Vigenere cipher cont.

- Key: KEY Message: SECRET TEXT

K	E	Y	K	E	Y	K	E	Y	K
S	E	C	R	E	T	T	E	X	T
C	I	A	B	I	R	D	I	V	D

- Still vulnerable to analytical attacks.
- **Question: Does an invulnerable cipher exist?**

Let me introduce to you now to the concept of 'confusion' and 'diffusion', which were formalized by Claude Shannon in his 1949 paper Communication Theory of Secrecy Systems. [26]

- 'Confusion' is the operation where the relationship of key and ciphertext is obscured.
- 'Diffusion' is the operation where the influence of one plaintext symbol is spread over many ciphertext symbols (Needed to hide statistical properties).

We've already seen 'confusion' in action with the Vigenère cipher. We'll see later on an example of 'diffusion'.

Next: The invulnerable cipher.

Encryption
└Cryptography
└Cryptosystems

Perfect secrecy

Claude Shanon (1949):

Definition
A cipher (E,D) defined over $(\mathcal{K},\mathcal{M},\mathcal{C})$ has perfect secrecy if

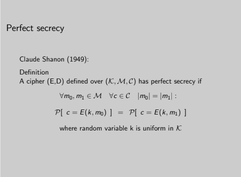
$$\forall m_0, m_1 \in \mathcal{M} \quad \forall c \in \mathcal{C} \quad |m_0| = |m_1| :$$

$$\mathcal{P}[\ c = E(k, m_0)\ ] \ = \ \mathcal{P}[\ c = E(k, m_1)\ ]$$

where random variable k is uniform in $\mathcal{K}$

2015-08-15

Encryption
└Cryptography
└Cryptosystems
└Perfect secrecy



Perfect secrecy

Claude Shanon (1949):

Definition
A cipher (E,D) defined over $(\mathcal{K},\mathcal{M},\mathcal{C})$ has perfect secrecy if

$$\forall m_0, m_1 \in \mathcal{M} \quad \forall c \in \mathcal{C} \quad |m_0| = |m_1| :$$

$$\mathcal{P}[\ c = E(k, m_0)\ ] \ = \ \mathcal{P}[\ c = E(k, m_1)\ ]$$

where random variable k is uniform in $\mathcal{K}$

An unbreakable cipher would be one that outputs ciphertexts, which an attacker has no way of decrypting with analytical attacks alone. Shannon mathematical definition of 'perfect secrecy' translates roughly as: Given a ciphertext c, the probability of that ciphertext being an encryption of a message m with a random key k is the same as the probability of that ciphertext coming from an encryption of any other message of the same length in the Plaintext-space with random key k.

(Claude Shanon, known as the father of information theory, was an American mathematician and engineer who developed Information Theory among other things.) [14]

Perfect secrecy of One-time-pad

One-time-pad has perfect secrecy.

Preliminaries:

$$\mathcal{P}[\ c = E(k,m)\ ] \ = \frac{|\ \{\ k \in \mathcal{K}\ |\ E(k,m) = c\ \}\ |}{|\mathcal{C}|}$$

$\otimes$: Vigenere encription operation. $\oslash$: V. decription op.

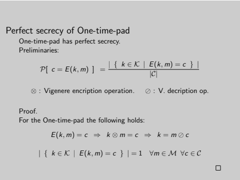
Proof.

For the One-time-pad the following holds:

$$E(k,m) = c \ \Rightarrow \ k \otimes m = c \ \Rightarrow \ k = m \oslash c$$

$$|\ \{\ k \in \mathcal{K}\ |\ E(k,m) = c\ \}\ | = 1 \quad \forall m \in \mathcal{M}\ \forall c \in \mathcal{C}$$

□



Perfect secrecy of One-time-pad
One-time-pad has perfect secrecy.
Preliminaries:
$\mathcal{P}[\ c = E(k,m)\ ] = \frac{|\ \{\ k \in \mathcal{K}\ |\ E(k,m) = c\ \}\ |}{|\mathcal{C}|}$
$\otimes$: Vigenere encription operation. $\oslash$: V. decription op.
Proof.
For the One-time-pad the following holds:
$E(k,m) = c \Rightarrow k \otimes m = c \Rightarrow k = m \oslash c$
$|\ \{\ k \in \mathcal{K}\ |\ E(k,m) = c\ \}\ | = 1 \quad \forall m \in \mathcal{M}\ \forall c \in \mathcal{C}$
□

The one-time pad is a special case of the Vigenère cipher were the key is as long as the message.

The one-time pad has perfect secrecy. (It's also called Vernam cipher for the Bell Labs engineer Gilbert Vernam. Later, Claude Shannon proved in 1949 that the one-time pad is unbreakable). [27]

There are a series of Requirements that the one-time pad must fullfill to maintain its perfect secrecy property:

- Key must be at least as long as the message (and must always be kept secret).
- The key must be generated randomly.
- The key can only be used once (Hence the name, one-time pad).

Note: In the proof, that the encryption and decryption algorithm are not the same (for example if the plaintext consist of symbols from the latin alphabet). In the case that we were dealing with bits, the encryption and decryption would be the same (XOR-operation).

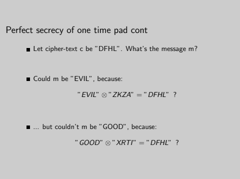
Perfect secrecy of one time pad cont

- Let cipher-text c be "DFHL". What's the message m?
- Could m be "EVIL", because:

$$\text{"}EVIL\text{"} \otimes \text{"}ZKZA\text{"} = \text{"}DFHL\text{"} \ ?$$

- ... but couldn't m be "GOOD", because:

$$\text{"}GOOD\text{"} \otimes \text{"}XRTI\text{"} = \text{"}DFHL\text{"} \ ?$$



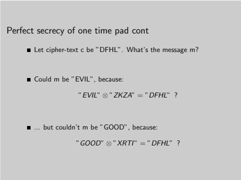
Perfect secrecy of one time pad cont
Let cipher-text c be "DFHL". What's the message m?
Could m be "EVIL", because:
"EVIL" $\otimes$ "ZKZA" = "DFHL" ?
... but couldn't m be "GOOD", because:
"GOOD" $\otimes$ "XRTI" = "DFHL" ?

Is the one-time pad truly impossible to break? Couldn't we with sufficient computing power find eventually the message that hides behind the ciphertext?

The one-time pad is, if used correctly, in all the sense of the word unbreakble. If we had enough time or unlimited computing power we would stumble not only on the message that we're looking for, but with all other possible messages in the Plaintext. To be more to the point: we wouldn't be able to distinguish the message we're looking for from all the other messages that are also when read, proper english sentences.

Without the key, it's impossible to gain any information with cipher-text-only attacks.

This is what truly means for a cipher to be information-theoretically secure. [7]



Perfect secrecy of one time pad cont

- Let cipher-text c be "DFHL". What's the message m?
- Could m be "EVIL", because:

$$"EVIL" \otimes "ZKZA" = "DFHL" \quad ?$$

- ... but couldn't m be "GOOD", because:

$$"GOOD" \otimes "XRTI" = "DFHL" \quad ?$$

One thing that stands out of the one-time pad is that it doesn't use any operation that adds 'confusion'. 'Confusion' means that each symbol of the ciphertext must depend on more than one part of the key. (If a symbol of the plaintext is changed, several parts of the ciphertext should change too, and vice versa). The one-time pad doesn't need to add confusion since its key is as long as the message.
Even though the one-time pad is unbreakable, it is very difficult to implement, because the key must be at least as long as the message. In fact, Shannon was even able to prove that all ciphers with perfect secrecy have a key at least as long as the message.
Since perfect secrecy ciphers are unpractical, we need other 'probably secure' ciphers. Such ciphers depend on operations that add 'confusion' as much as 'diffusion'.

But how is 'confusion' even possible? Our upcoming and last cipher is a good example.

Playfair Cipher

m = CIA BIRD

k=PASSWORD

p	a	s	w	o
r	d	b	c	e
f	g	h	i	j
k	l	m	n	q
t	u	v	x	yz

$$m = CI \quad AB \quad IR \quad DX$$
$$c = IN \quad SD \quad FC \quad CU$$

Playfair Cipher

m = CIA BIRD

k=PASSWORD

p	a	s	w	o
r	d	b	c	e
f	g	h	i	j
k	l	m	n	q
t	u	v	x	yz

$$m = CI \quad AB \quad IR \quad DX$$
$$c = IN \quad \cdot\cdot \quad \cdot\cdot \quad \cdot\cdot$$

Playfair Cipher

m = CIA BIRD

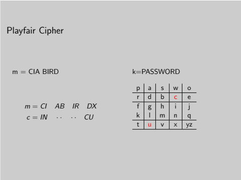
k=PASSWORD

p	a	s	w	o
r	d	b	c	e
f	g	h	i	j
k	l	m	n	q
t	u	v	x	yz

$$m = CI \quad AB \quad IR \quad DX$$
$$c = IN \quad \cdot\cdot \quad \cdot\cdot \quad CU$$

2015-08-15

Encryption
└Cryptography
└Cryptosystems
└Playfair Cipher



Playfair Cipher

m = CIA BIRD

$m = CI \quad AB \quad IR \quad DX$
$c = IN \quad \cdot\cdot \quad \cdot\cdot \quad CU$

k=PASSWORD

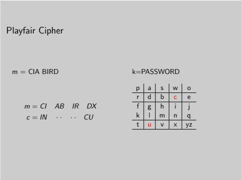
p	a	s	w	o
r	d	b	c	e
f	g	h	i	j
k	l	m	n	q
t	u	v	x	yz

With the message 'CIABIRD' and password 'PASSWORD' we would obtain the ciphertext 'INSDFCCU'. The implementation details follow: This cipher consist of a 5x5 table: You start writing first the key in the table and omitting letters already written (In our example: 'password' we would write first pasword, with only one 's', since it has been already included). And then we fill the rest of the table with the letters of the alphabet in order such that no letter is found twice in the table. If the key is too short, like in our case we'll have to put 2 or more less frequent letters in one space (We took 'y' and 'z').
Before encrypting, separate the letters of the message into groups of 2. One encrypts 2 letters at a time following 4 simple rules [21]:

- If the two letters are the same, put an 'x' or other unfrequent letter between them. And start again.
- If the letter are on the same column, encrypt each letter with the one underneath.
- If on the same row, encrypt each letter with the one to the right.
- Else they'll form a rectangle. (See slide).

2015-08-15

Encryption
└Cryptography
└Cryptosystems
└Playfair Cipher



Playfair Cipher

m = CIA BIRD

$m = CI \quad AB \quad IR \quad DX$
$c = IN \quad \cdot\cdot \quad \cdot\cdot \quad CU$

k=PASSWORD

p	a	s	w	o
r	d	b	c	e
f	g	h	i	j
k	l	m	n	q
t	u	v	x	yz

Although the playfair cipher has not practical use for todays ciphers, it is a good text-book example of how 'diffusion' can be achieved.
(If we changed one letter in the message, we would change one and potentially even more letters in the ciphertext).
Hisorical note: The Playfair-cipher was invented in 1854 by english scientist Charles Wheatstone, but bears the name of Lord Playfair, scottish scientist and politician, who promoted the use of the cipher. [21]

Encryption
└Cryptography
└Cryptosystems

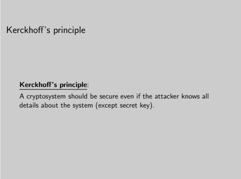
Kerckhoff's principle

Kerckhoff's principle:

A cryptosystem should be secure even if the attacker knows all details about the system (except secret key).

2015-08-15

Encryption
└Cryptography
└Cryptosystems
└Kerckhoff's principle



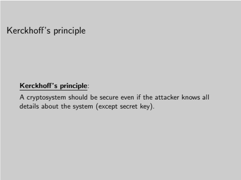
Kerckhoff's principle

Kerckhoff's principle:
A cryptosystem should be secure even if the attacker knows all details about the system (except secret key).

This principle was coined by dutch linguist and cryptographer Auguste Kerckhoffs in the second half of the 19th century. It is embraced nowadays by many cryptographers and scientists alike. It can be seen as a response to the belief of "security through obscurity". [29, p.11]
It is a very simple principle and yet very unintuitive: History has taught us that trying to hide the workings of crypto-systems are a rather bad approach in making them. There are numerous example where one thinks that an encryption algorithm is secure, when there are actually ways of breaking the system and compromising information.

2015-08-15

Encryption
└─Cryptography
  └─Cryptosystems
    └─Kerckhoff's principle


Kerckhoff's principle

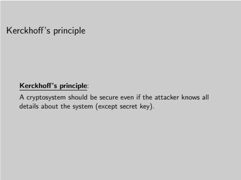
Kerckhoff's principle:
A cryptosystem should be secure even if the attacker knows all details about the system (except secret key).

Short example of "Security through obscurity": The germans used during the WWII a machine called enigma to encrypt their communications. Polish secret intelligence 1927 got hold of such a mashine, when it was still possible to buy one. They achieved in 1938 to decrypt the machine with another machine, which they called Bomba (name comes from an ice-cream dessert). The germans used more than 50 different enigmas and made a lot of improvements in their machines. The british intelligence, with cooperation of the polish, gathered a team composed of linguists, mathematicians, among them Alan Turing, to break the enigma machine. They improved the polish machine considerably and made it possible to decrypt the germans messages. [31]

Small note: One technical reason that made the enigma machine possible to break was that it only used 'confusion' in their encryption. (It lacked 'diffusion'). [29, p.57]

2015-08-15

Encryption
└─Cryptography
  └─Cryptosystems
    └─Kerckhoff's principle


Kerckhoff's principle

Kerckhoff's principle:
A cryptosystem should be secure even if the attacker knows all details about the system (except secret key).

Cryptography has been for a long time and is still nowadays a cat and mouse game.

Kerckhoff's principle can be seen as a method of using history itself to help us improve and construct better ciphers. It is always with the help of cryptoanalysts that better ciphers have been constructed.

Reverse-engineering an encryption algorithm has proven to be easier than it's at first intuitively thought. Today a cipher is only as good as the time it has spent unbroken and on scrutiny by todays best cryptoanalysts.

Encryption
└─Modern examples
  └─CSS DVD

DVD content protection

- Used to:
  - protect against piracy
  - enforce regional restrictions
- Streamcipher
- Key length: 40 bits.
- Broken without a brute-force approach.

2015-08-15

Encryption
└─Modern examples
  └─CSS DVD
    └─DVD content protection

DVD content protection

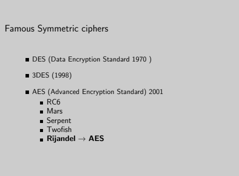
- Used to:
  - protect against piracy
  - enforce regional restrictions
- Streamcipher
- Key length: 40 bits.
- Broken without a brute-force approach.

CSS is a cryptoauthentication system between DVD disc and the DVD player [15]. An organization, DVD CCA (DVD Copy Control Association), had the task of distributing keys to the DVD player manufacturers (Examples: Sony, Panasonic, etc). Keys are given as carefully as it was possible. Decrypting hardware is installed to the DVD player and the key is hard-coded in. It is more difficult to find keys coded in hardware than in software. The problem with CSS was that the cryptosystem and keys had to remain secret. Things didn't go as expected for those interested in the encryption: secrets leaked and someone cracked the system. 15-year-old norway student Jon Johansen and a group of german hackers developed a software program called DeCSS. Soon norwegian authorities knocked on Johansens door, took his computers and cell phone, and took him out for questioning.

Today, CSS is seen as breakable, not only for the leaked information about its keys and hardware, but because of the short key itself. [1]

Famous Symmetric ciphers

- DES (Data Encryption Standard 1970)
- 3DES (1998)
- AES (Advanced Encryption Standard) 2001
  - RC6
  - Mars
  - Serpent
  - Twofish
  - **Rijandel → AES**

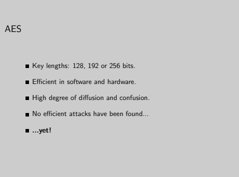


Famous Symmetric ciphers
DES (Data Encryption Standard 1970)
3DES (1998)
AES (Advanced Encryption Standard) 2001
RC6
Mars
Serpent
Twofish
Rijandel → AES

DES, data encryption standard , was for 30 years the predominant symmetric-key algorithm for the encryption. It was developed in the early 1970s at IBM. (Controversy: Improper interference from the NSA?) [16]
Already in the late 90's DES was considered to be insecure for a wide range of applications, mainly due to the 56-bit key size being too small. Alternatives at that time were 3DES, which, as the name hints, involved running DES three times in a row on the data. Efficiency was the problem.
The US National Institute of Standards and Technology organized an open, transparent process for selecting the new Advanced Encryption Standard (AES) that would replace DES. Many of the finalists listed on the slide can be used today as means of encryption. The winners of that process was the Rijandel algorith of belgian cryptographers Joan Daemen and Vincent Rijmen. [29, p.88-90]

AES

- Key lengths: 128, 192 or 256 bits.
- Efficient in software and hardware.
- High degree of diffusion and confusion.
- No efficient attacks have been found...
- **...yet!**

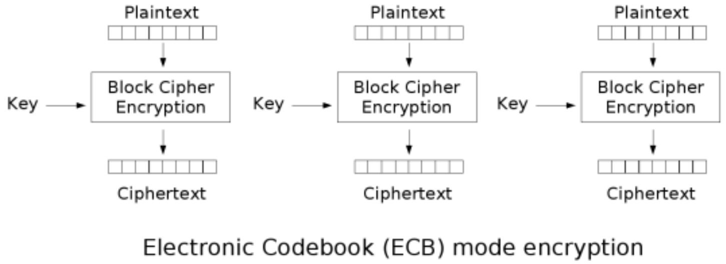


AES
Key lengths: 128, 192 or 256 bits.
Efficient in software and hardware.
High degree of diffusion and confusion.
No efficient attacks have been found...
...yet!

This symmetric-key algorithm is widely used today for many commercial applications and since 2003 (surprisingly) by the NSA to encrypt documents classified as 'secret' and for documents classified as 'top secret' (but only with 192 or 256 bit keys). [29, p.89]

Encryption modes

- ECB (Electronic Code Book)

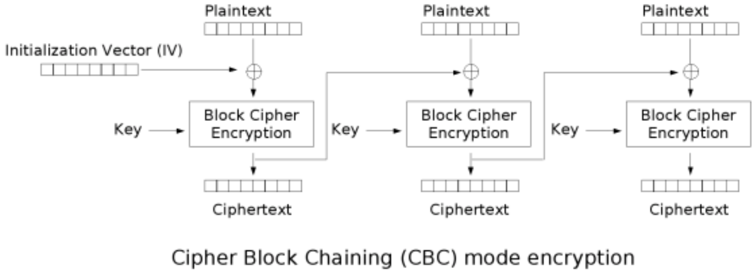


Electronic Codebook (ECB) mode encryption

Figure : [9]

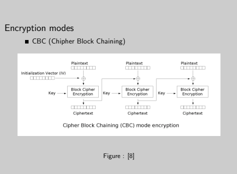
Encryption modes

- CBC (Chipher Block Chaining)



Cipher Block Chaining (CBC) mode encryption

Figure : [8]



Of course, we don't want to encrypt every 128 bits with a new key. That is why we need block ciphers.
ECB and CBC are among the most common modes of encryption available for block ciphers. [29, p.124]
One of ECB advantages are that if not all blocks were transmitted (because of some transmission problem), it is still possible to decrypt the blocks that were recieved. Encryption can also be parrallelised. But ECB doesn't hide data patterns well, because all identical block codes will be encrypted the same way.
CBS uses an itialization vector, a pseudo-random sequence of bits the size of the block length, that is used to XOR the first block. It is most commonly used for encryption, with the only disadvantage that is cannot be parallelised since the encryption of one block depends on the encryption of the following block (decryption can be parrallized).
Speaking only in terms of security, CBS is a much more secure block cipher than ECB.

Hardware-based encryption

- No performance overhead.
- Transparency.
- HDD/SDDs vendors: disk controller.
- IBMs: Secure Blue
- Encrypt entire boot disk and MBR.

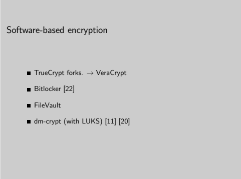
Hardware-based encryption

- No performance overhead.
- Transparency.
- HDD/SDDs vendors: disk controller.
- IBMs: Secure Blue
- Encrypt entire boot disk and MBR.

For a full list see: [17]
Transparency, accomplished by on-the-fly encryption, is a feature that many encryption hardware offer. Transparency means that the data is automatically encrypted/decrypted as it is loaded/stored.
Some full-disk encryption hardware are able to encrypt not only the entire disk but also the master boot record.
The boot key problem: How can the user give the password when the OS is encrypted? A pre-boot authentication environment has to be created to solve this problem.
[2]

Software-based encryption

- TrueCrypt forks. → VeraCrypt
- Bitlocker [22]
- FileVault
- dm-crypt (with LUKS) [11] [20]



Software-based encryption

- TrueCrypt forks. → VeraCrypt
- Bitlocker [22]
- FileVault
- dm-crypt (with LUKS) [11] [20]

For a full list see [18].
Many users today look at TrueCrypt with nostalghia. In may of 2014 this software, that supported many encryption algorithms like AES, Serpent, and Twofish and even offered cascading, was discontinued and can not be counted as secure. There are many forks of it, with the most common one today being VeraCrypt. [24]
Bitlocker, appeared for the first time in some versions of Windows Vista, and is capable of full disk encryption. It uses the AES algorithm in cipher block chaining mode (CBC) with a 128 or 256 key and some additional features. Note: CBC is not used on the complete disk, but on each individual disk sector independently. (Nowadays to be found in some versions of Windows 7 and 8). [22]
FileVault is the disk encryption software for mac computers. Encryption and decryption are performed on the fly.

Summary

- Kerckhoff's Principle
- Encryption done right depends on:
  - Keyspace
  - Good algorithm (cipher)
  - Implementation
- A secure cipher uses...
  - Confusion
  - Diffusion

Bibliography I

[1] *Cryptography in home entertainment a look at content scrambling in dvds*, http://www.math.ucsd.edu/~crypto/Projects/MarkBarry/.

[2] *Disk encryption*, http://en.wikipedia.org/wiki/Disk_encryption.

[3] *Disk encryption theory*, http://en.wikipedia.org/wiki/Disk_encryption_theory.

[4] *Hardware-based full disk encryption*, http://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption.

[5] *Luks and cryptsetup*, https://gitlab.com/cryptsetup/cryptsetup.

[6] *Performance analysis of data encryption algorithms*, http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/.

[7] *en.wikipedia.org/wiki/Information_theory*.

Bibliography II

[8] *http://commons.wikimedia.org/wiki/File:Cbc_encryption.png*.

[9] *http://commons.wikimedia.org/wiki/File:Ecb_encryption.png*.

[10] *http://de.wikipedia.org/wiki/Betriebsmodus_Kryptographie*.

[11] *http://de.wikipedia.org/wiki/Dm-crypt*.

[12] *http://de.wikipedia.org/wiki/Kryptographie*.

[13] *http://de.wikipedia.org/wiki/Verschluesselung*.

[14] *http://en.wikipedia.org/wiki/Claude_Shannon*.

[15] *http://en.wikipedia.org/wiki/Content_Scramble_System*.

[16] *http://en.wikipedia.org/wiki/Data_Encryption_Standard*.

Bibliography III

[17] *http://en.wikipedia.org/wiki/Disk_encryption_hardware*.

[18] *http://en.wikipedia.org/wiki/Disk_encryption_software*.

[19] *http://en.wikipedia.org/wiki/Encrypting_File_System*.

[20] *http://en.wikipedia.org/wiki/Linux_Unified_Key_Setup*.

[21] *http://en.wikipedia.org/wiki/Playfair_cipher*.

[22] *https://en.wikipedia.org/wiki/BitLocker*.

[23] *https://en.wikipedia.org/wiki/Encryption*.

[24] *https://en.wikipedia.org/wiki/TrueCrypt*.

[25] *Vigenere cipher online*, http://rumkin.com/tools/cipher/vigenere.php.

Bibliography IV

[26] *Wiki: Confusion and diffusion*, http://en.wikipedia.org/wiki/Confusion_and_diffusion.

[27] Dan Boneh, *Cryptography i*, Coursera.org, Online Stanford course Video lecture series 1 and 2.

[28] Markus Mandau, *Richtig verschluesseln*, Chip (2015).

[29] Christoph Paar and Jan Pelzl, *Understanding cryptography*, first ed., Springer Verlag, 2010.

[30] Christian Ney Peter Gutmann, *Löchriger käse*, http://www.linux-magazin.de/Ausgaben/2006/10/Loechriger-Kaese, Linux Magazin.

[31] Klaus Schmeh, *Kryptographie, verfahren, protokollen, infrastrukturen*, dpunkt.verlag, 2007.

[32] Alexander Stanoyevitch, *Introduction to cryptography with mathematical foundations and computer implementations*, first ed., CRC Press, 2011.