Encryption

Nicolaus Moeller

Studiengang Informatik
Universität Hamburg

June 10, 2015

Contents

Motivation

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

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

Problem

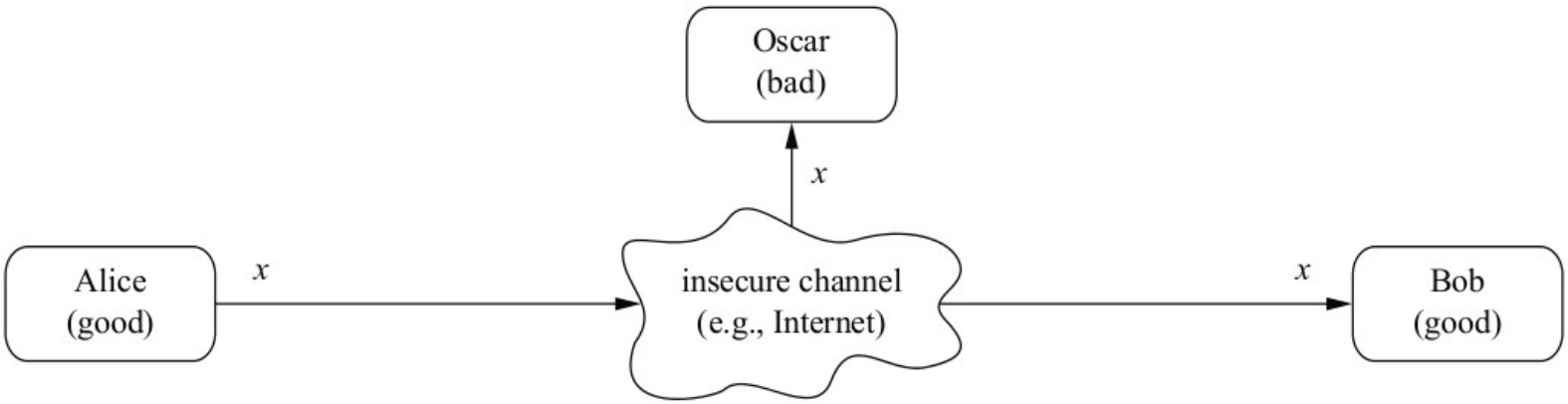


Figure : [26, p.5]

Problem

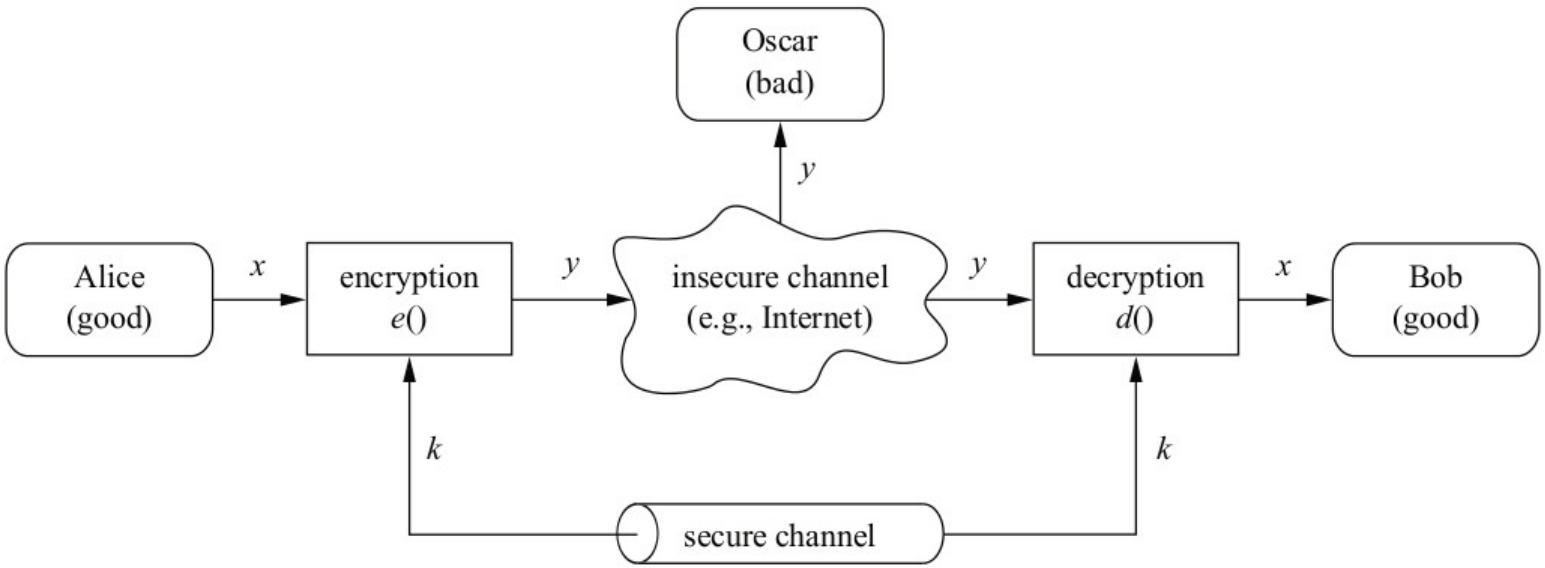


Figure : [26, p.5]

Cryptology

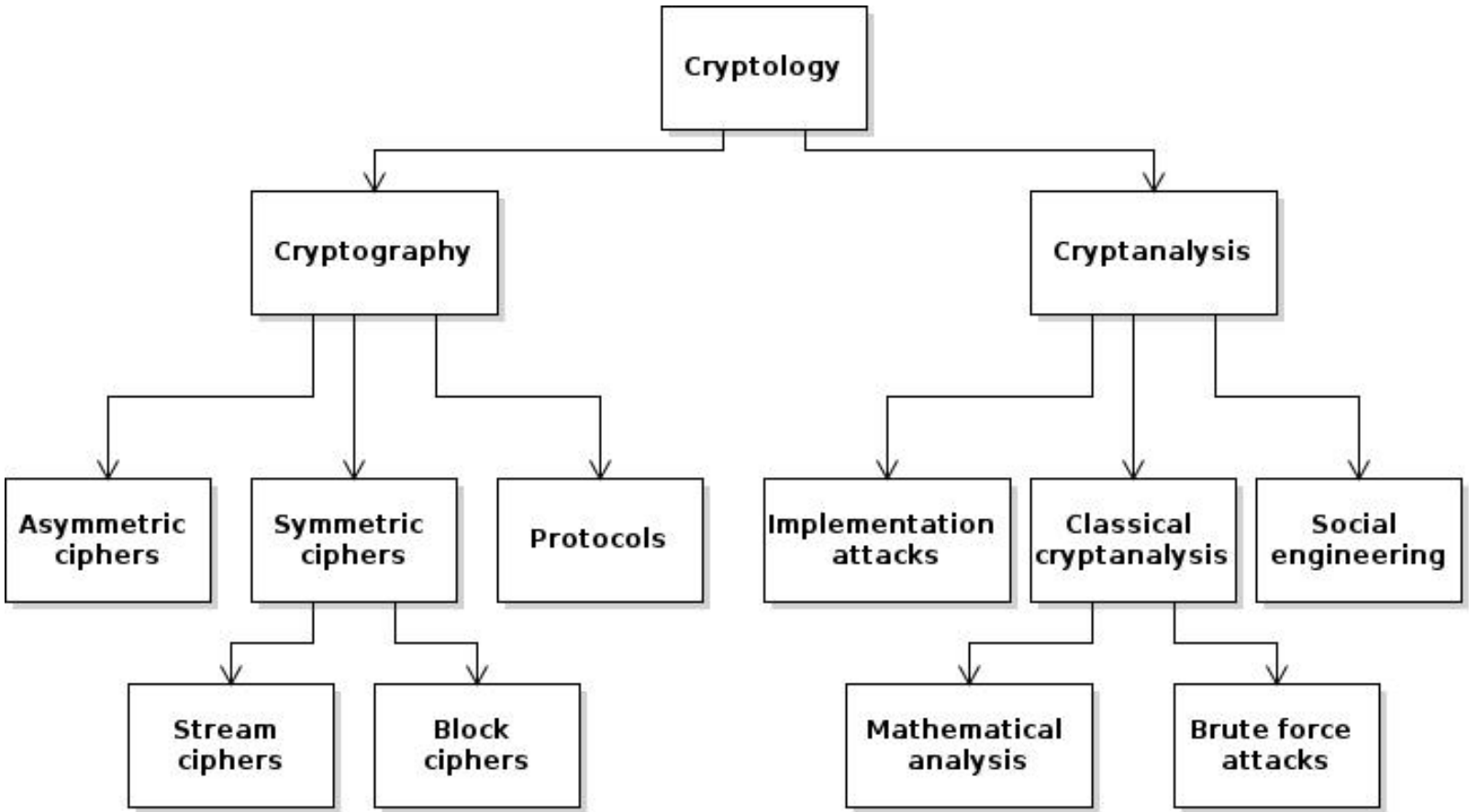


Figure : [26, p.3 and 10]

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

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

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

Question: What is a good cipher?

Substitution cipher

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

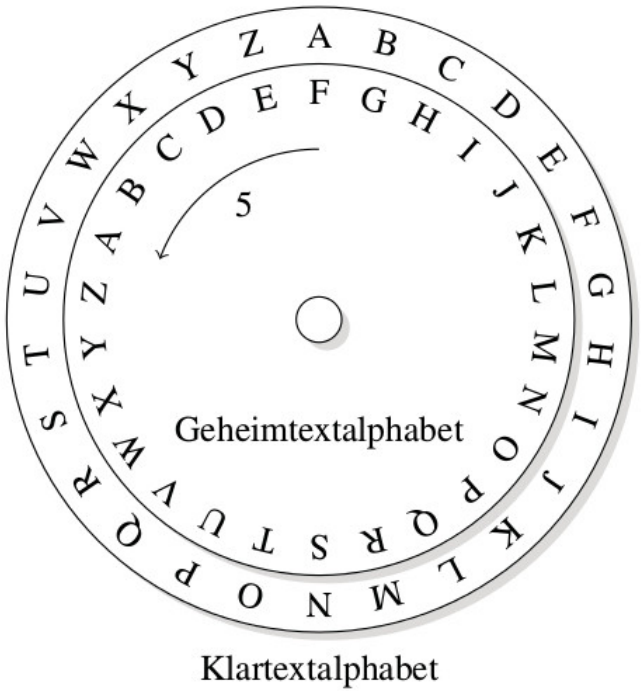


Figure : [26, p.9]

Substitution cipher cont.

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

- Very unsecure!

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 : [26, p.9]

- Very unsecure!

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 : [26, p.9]

- Very unsecure!

Vigenere cipher

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

- Encrypt using modular arithmetic

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

$$(17 + 23) \equiv 40 \equiv 14 \bmod 26$$

Result: $O \rightarrow 14$

- Decryption:

$$(14 - 23) \equiv -9 \equiv 17 \bmod 26$$

Vigenere cipher

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

- Encrypt using modular arithmetic

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

$$(17 + 23) \equiv 40$$
$$\equiv 14 \bmod 26$$

Result: $O \rightarrow 14$

- Decryption:

$$(14 - 23) \equiv -9$$
$$\equiv 17 \bmod 26$$

Vigenere cipher

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

- Encrypt using modular arithmetic

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

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

Result: $O \rightarrow 14$

- Decryption:

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

Vigenere cipher

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

- Encrypt using modular arithmetic

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

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

  Result: $O \rightarrow 14$

- Decryption:

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

Vigenere cipher cont.

- Key: KEY Message: SECRET TEXT

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

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

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.

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?**

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 $\mathcal{K}$

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 $\mathcal{K}$

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 $\mathcal{K}$

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:

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

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

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 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:

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

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:

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

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:

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

Playfair Cipher

m = CIA BIRD

k=PASSWORD

Playfair Cipher

m = CIA BIRD

$m = CI \quad AB \quad IR \quad DX$

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

Playfair Cipher

m = CIA BIRD

$m = CI \quad AB \quad IR \quad DX$

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

Playfair Cipher

m = CIA BIRD

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

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

Playfair Cipher

m = CIA BIRD

$m = CI \quad AB \quad IR \quad DX$

$c = IN \quad .. \quad .. \quad ..$

k=PASSWORD

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

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

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

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

$m = CI \quad AB \quad IR \quad DX$

$c = IN \quad SD \quad FC \quad CU$

Kerckhoff's principle

Kerckhoff's principle:

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

DVD content protection

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

Famous Symmetric ciphers

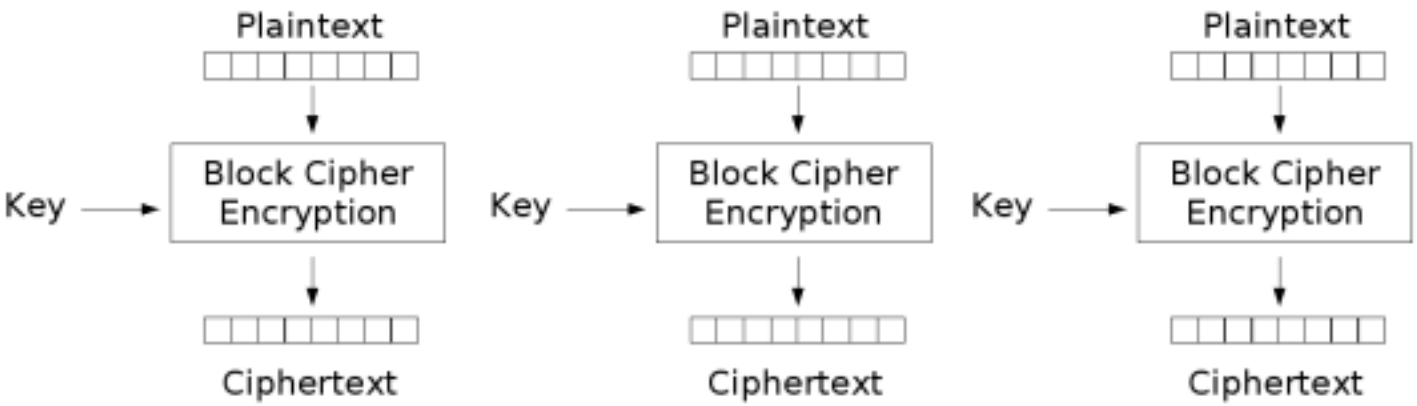
- DES (Data Encryption Standard 1970)
- 3DES (1998)
- AES (Advanced Encryption Standard) 2001
  - RC6
  - Mars
  - Serpent
  - Twofish
  - **Rijandel** $\rightarrow$ **AES**

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!**

Encryption modes

- ECB (Electronic Code Book)

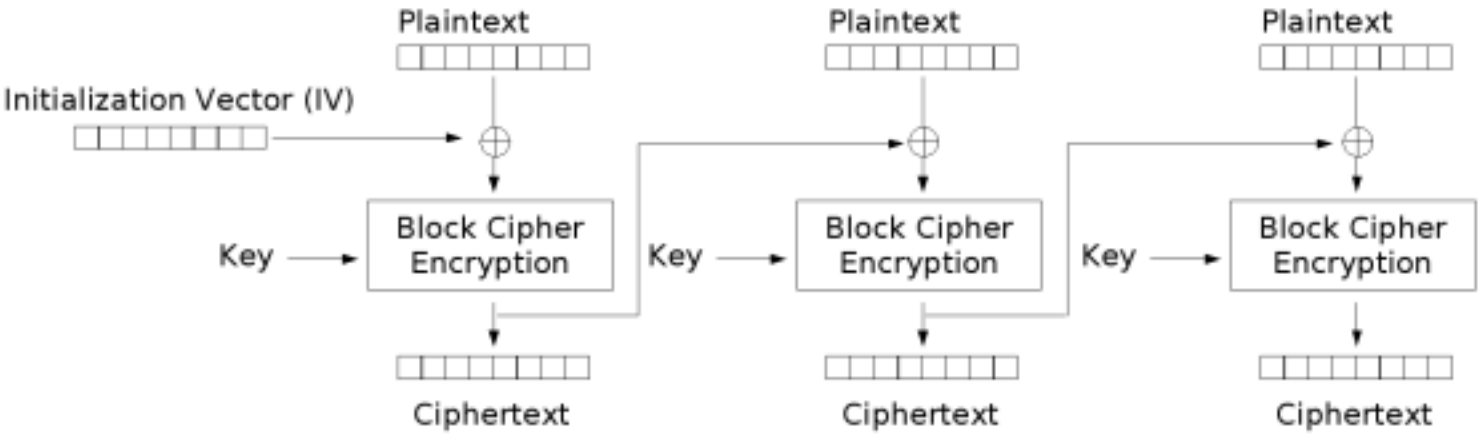


Electronic Codebook (ECB) mode encryption

Figure : [9]

Encryption modes

- CBC (Chipher Block Chaining)



Cipher Block Chaining (CBC) mode encryption

Figure : [8]

Hardware-based encryption

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

Software-based encryption

- TrueCrypt forks. $\rightarrow$ VeraCrypt
- Bitlocker
- FileVault
- dm-crypt (with LUKS)

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

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

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

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

Bibliography IV

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

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

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

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