

Symmetrisk kryptografi

Daniel Bosk¹

Avdelningen för informations- och kommunikationssystem (IKS),
Mittuniversitetet, Sundsvall.

symcrypt.tex 1313 2013-09-20 17:57:19Z danbos

¹Detta verk är tillgängliggjort under licensen Creative Commons Erkännande-DelaLika 2.5 Sverige (CC BY-SA 2.5 SE). För att se en sammanfattning och kopia av licenstexten besök URL
<http://creativecommons.org/licenses/by-sa/2.5/se/>

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Litteratur

The lecture essentially covers “En introduktion till kryptografi” [Bos13], chapter 2 “Symmetric Encryption and Message Confidentiality” in *Network security essentials : applications and standards* [Sta13], and chapter 5 “Cryptography” in *Security engineering : a guide to building dependable distributed systems* [And08].

You should then solve problems 2.1, 2.2, 2.12, 2.13 and 2.14 in [Sta13].



Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Översikt

1 Klassisk kryptografi

- **Kryptosystem**
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

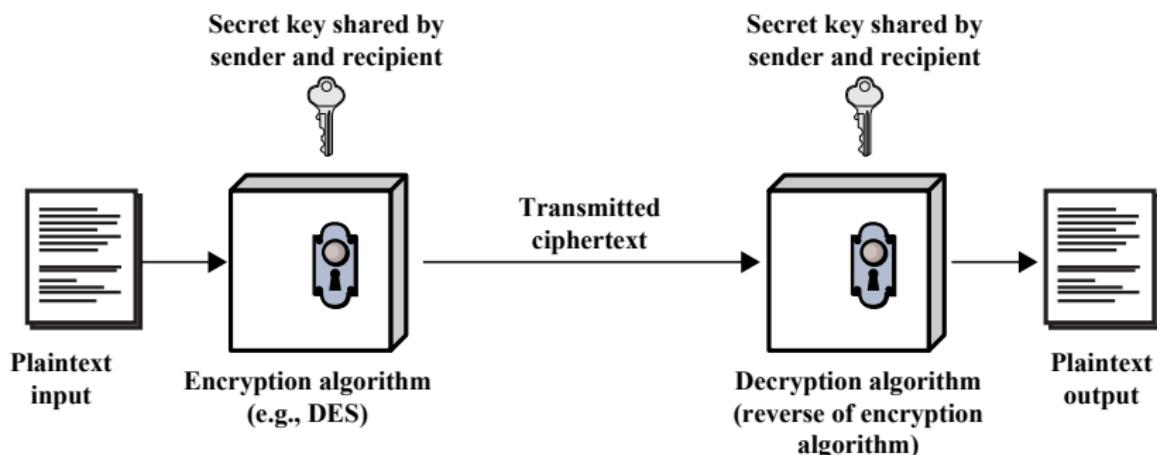
4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Kryptosystem

- Ordet kryptografi kommer från grekiskans $\chiρυπτός$ (*kryptos*) och $\gammaράφος$ (*graphos*) [OED2013cg].
 - Dessa betyder *gömd* eller *hemlig* [OED2013c] respektive *skrift* [OED2013g].
 - Ordet kryptografi betyder följaktligen *hemlig skrift*.
 - I modern tid är kryptografin ett högst matematiskt område.
 - Det finns inte utrymme för annat än matematisk precision.

Kryptosystem



Figur : Symmetrisk kryptering. Bild: [Sta11].

Kryptosystem

Definition

Ett kryptosystem är en tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ där följande gäller:

- ① \mathcal{P} är en ändlig mängd av möjliga klartexter.
 - ② \mathcal{C} är en ändlig mängd av möjliga kryptotexter.
 - ③ \mathcal{K} , kallad *nyckelrymden*, är en ändlig mängd av möjliga nycklar.
 - ④ För varje $k \in \mathcal{K}$ finns en *krypteringsregel* $e_k \in \mathcal{E}$ och motsvarande *avkrypteringsregel* $d_k \in \mathcal{D}$. Varje $e_k: \mathcal{P} \rightarrow \mathcal{C}$ och $d_k: \mathcal{C} \rightarrow \mathcal{P}$ är funktioner sådana att $d_k(e_k(p)) = p$ för alla klartexter $p \in \mathcal{P}$.

Kryptosystem

- Typer av operationer för att transformera klartext till kryptotext.
- Antalet nycklar som används.
- Sätt att processa klartexten:
 - Blockchiffer.
 - Strömchiffer.

Kryptosystem

Kryptanalys

- Enbart chiffertext (ciphertext only).
- Känd klartext (known plaintext).
- Vald klartext (chosen plaintext).
- Vald kryptotext (chosen ciphertext).
- Vald text (chosen text).

Kryptosystem

Definition

Ett kryptosystem är beräkningsmässigt säkert om det uppfyller någon eller båda av följande:

- Kostnaden för att knäcka chiffret är högre än värdet på informationen det skyddar.
- Tiden det tar att knäcka chiffret är längre än tiden informationen är värdefull.



Översikt

1 Klassisk kryptografi

- Kryptosystem
- **Substitutionschiffer**
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Substitutionschiffer

Caesarchiffer

Definition (Skiftchiffer)

Låt $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{29}$ och låt varje bokstav i det svenska alfabetet motsvara ett unikt tal i \mathbb{Z}_{29} . För alla $k \in \mathcal{K}$ definierar vi

$$\begin{aligned} e_k(p) &= (p + k) \text{ mod } 29, \text{ och} \\ d_k(c) &= (c - k) \text{ mod } 29, \end{aligned}$$

där $p \in \mathcal{P}$ är en klartextbokstav och $c = e_k(p) \in \mathcal{C}$ är motsvarande kryptotextbokstav.



Substitutionschiffer

Caesarchiffer

Exempel

Låt oss numrera bokstäverna i det svenska alfabetet enligt index med start från noll. Då får vi att textsträngen "hej" skulle kunna motsvaras av tupeln $p = (7, 4, 9)$. Om vi låter nyckeln $k \in \mathcal{K}$ vara 2 får vi att

$$\begin{aligned}c &= e_2(p) = (e_2(7), e_2(4), e_2(9)) \\&= (9, 6, 11).\end{aligned}$$

Om vi översätter tillbaka till bokstäver får vi att c motsvarar strängen "JGL".

Exempel

Om vi krypterar ordet *skatten* blir det *UMCVVGP*.

Substitutionschiffer

Caesarchiffer

Kryptanalys

- Kan enkelt testa alla 29 nycklarna för hand.
- Kan titta efter upprepningar:
 - Upprepade bokstäver är sannolikt konsonanter.
 - Upprepade bokstavskombinationer är sannolikt vanliga ord.
- Trots enkelheten att knäcka detta försökte terrorister seriöst att använda systemet så sent som 2011 [[Register2011bjr](#)].



Substitutionschiffer

Definition (Substitutionschiffer)

Låt A vara vårt alfabet och låt $\mathcal{P} = \mathcal{C} = A$. Vidare låt \mathcal{K} bestå av alla möjliga permutationer av A . För varje permutation $\pi \in \mathcal{K}$ definierar vi att

$$\begin{aligned} e_\pi(p) &= \pi(p), \text{ och} \\ d_\pi(c) &= \pi^{-1}(c), \end{aligned}$$

där π^{-1} är den inverterade permutationen π , $p \in \mathcal{P}$ är en klartextbokstav och $c = e_\pi(p) \in \mathcal{C}$ är motsvarande kryptotextbokstav.



Substitutionschiffer

α	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
$\pi(\alpha)$	C	M	Q	F	Z	Ö	I	J	P	L	D	N	O	K	D
α	p	q	r	s	t	u	v	w	x	y	z	å	ä	ö	
$\pi(\alpha)$	R	S	T	Å	V	Y	X	W	G	U	Ä	H	A	B	

Tabell : Nyckel för att kryptera med ett substitutionschiffer. Gemener används som klartextalfabete och versaler som kryptoalfabete.

Substitutionschiffer

Exempel

Vi låter A vara det svenska alfabetet. Nyckeln $\pi \in \mathcal{K}$ ges av föregående tabell. Då får vi att $e_\pi(h) = J$, $e_\pi(e) = Z$, $e_\pi(j) = L$.

Exempel

Om vi krypterar ordet *skatten* blir det *ÅDCVVZK*.

Substitutionschiffer

$\Pr(X = \alpha)$	a 0.063	b 0.000	c 0.000	d 0.031	e 0.156	f 0.000	g 0.031	h 0.094	i 0.064	j 0.000
$\Pr(X = \alpha)$	k 0.000	l 0.063	m 0.000	n 0.094	o 0.031	p 0.000	q 0.000	r 0.031	s 0.156	t 0.125
$\Pr(X = \alpha)$	u 0.000	v 0.000	w 0.031	x 0.031	y 0.000	z 0.000	å 0.000	ä 0.000	ö 0.000	

Tabell : Tabell av sannolikhetsfördelningen för den stokastiska variabeln X som antar bokstäver i meningens "anenglishtexthasnoswedishletters", angiven med tre decimalers noggrannhet.



Substitutionschiffer

Sannolikhetsfördelningar

- Likformig sannolikhetsfördelning (uniform distribution).
- Oberoende.

Substitutionschiffer

α	A	B	C	D	E	F	G	H	I	J
$\Pr(Y = \alpha)$	0.000	0.000	0.063	0.000	0.000	0.031	0.156	0.000	0.031	0.094
α	K	L	M	N	O	P	Q	R	S	T
$\Pr(Y = \alpha)$	0.064	0.000	0.000	0.063	0.000	0.094	0.031	0.000	0.000	0.031
α	U	V	W	X	Y	Z	Å	Ä	Ö	
$\Pr(Y = \alpha)$	0.156	0.125	0.000	0.000	0.031	0.031	0.000	0.000	0.000	

Tabell : Tabell av sannolikhetsfördelningen för den stokastiska variabeln Y som antar bokstäver i meningens "CPGPINKUJVGZVJCUPQUYGFKUJNGVVGTU", angiven med tre decimalers noggrannhet.

Substitutionschiffer

Vigenèrehiffer

Definition (Vigenèrehiffer)

Låt n vara ett positivt heltal. Definiera att $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{29})^n$.

För alla nycklar $k = (k_1, \dots, k_n) \in \mathcal{K}$, klartexter

$p = (p_1, \dots, p_n) \in \mathcal{P}$ och kryptotexter $c = (c_1, \dots, c_n) \in \mathcal{C}$
definierar vi att

$$e_k(p) = (p_1 + k_1, \dots, p_n + k_n), \text{ och}$$

$$d_k(c) = (c_1 - k_1, \dots, c_n - k_n),$$

där alla operationer utförs i \mathbb{Z}_{29} .



Substitutionschiffer

Vigenèrechiffer

Klartext	a	b	c	d	e	f	g	h	i	j
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L

Klartext	k	l	m	n	o	p	q	r	s	t
A	K	L	M	N	O	P	Q	R	S	T
B	L	M	N	O	P	Q	R	S	T	U
C	M	N	O	P	Q	R	S	T	U	V

Klartext	u	v	w	x	y	z	å	ä	ö
A	U	V	W	X	Y	Z	Å	Ä	Ö
B	V	W	X	Y	Z	Å	Ä	Ö	A
C	W	X	Y	Z	Å	Ä	Ö	A	B

Tabell : Vigenèrechiffer med nyckeln ABC.

Substitutionschiffer

Vigenèrecipher

Exempel

Om vi vill kryptera orden *skatten* ska bokstäverna i nyckeln användas enligt

skatten

ABCABCA

och vi får alltså *SLCTUGN* genom att använda de olika Caesarchiffren i föregående tabell.

Substitutionschiffer

Vigenèrehiffer

Exempel

Ett Vigenèrehiffer med nyckeln *ABCD* används för att kryptera texten *cryptoisshortforcryptography*.

Nyckel: ABCDABCDABCDABCDABCDABCDABCD

Klartext: *cryptoisshortforcryptography*

Kryptotext: CSASTPKVSIQUTGQUCSASTPIUAQJB

Avståndet mellan den upprepade texten *CSASTP* är 16, från första tecken till första tecken. De möjliga nyckellängderna är alltså 16, 8, 4, 2 eller 1.

Substitutionschiffer

Vigenèrechiffer

Exempel

Ett Vigenèrechiffer med nyckeln *ABCD* används för att kryptera texten *cryptoisshortforcryptography*.

Nyckel:	ABCD	ABCD	
Klartext:	cryp	Kryptotext:	CSAS
	tois		TPKV
	shor		SIQU
	tfor		TGQU
	cryp		CSAS
	togr		TPIU
	aphy		AQJB

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer**
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Permutationschiffer

Definition (Permutationschiffer)

Låt n vara ett positivt heltal och A ett alfabet. Låt också $\mathcal{P} = \mathcal{C} = A^n$ och låt \mathcal{K} vara alla möjliga permutationer av mängden $\{1, \dots, n\}$. För en permutation $\pi \in \mathcal{K}$ definierar vi

$$e_\pi(p_1, \dots, p_n) = (p_{\pi(1)}, \dots, p_{\pi(n)}),$$

för alla klartexter $p = (p_1, \dots, p_n) \in \mathcal{P}$, och

$$d_\pi(c_1, \dots, c_n) = (c_{\pi^{-1}(1)}, \dots, c_{\pi^{-1}(n)}),$$

för alla kryptotexter $c = (c_1, \dots, c_n) \in \mathcal{C}$ och där π^{-1} är den inverterade permutationen π .

Permutationschiffer

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(i)$	1	8	2	9	3	10	4	11	5	12	6	13	7	14

Tabell : Definitionen av permutationen π .

Exempel

Låt $n = 14$. Permutationen $\pi \in \mathcal{K}$ definieras enligt tabellen ovan.

För att kryptera använder vi $e_\pi \in \mathcal{E}$. Om vi låter $p = (p_1, \dots, p_n)$ vara vår klartext "en dag i juni", får vi att

$c = e_\pi(p) = (p_1, p_8, p_2, p_9, \dots, p_7, p_{14})$ och således att c är vår kryptotext "EIN__JDUANGI__".

Vi avkrypterar på samma sätt med hjälp av π^{-1} .

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- **Perfekt sekretess**

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Perfekt sekretess

Definition

Ett kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ sägs ha *perfekt sekretess* om $\Pr(\mathbf{P} = p \mid \mathbf{C} = c) = \Pr(\mathbf{P} = p)$ för alla $p \in \mathcal{P}$ och $c \in \mathcal{C}$. Det vill säga, sannolikheten a posteriori att en klartext är p om kryptotexten är c är densamma som sannolikheten a priori att klartexten är p .

Perfekt sekretess

Sats (Shannons sats)

Antag att $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ är ett kryptosystem sådant att $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. Detta kryptosystem tillhandahåller perfekt sekretess om och endast om varje nyckel $k \in \mathcal{K}$ används med lika sannolikhet $1/|\mathcal{K}|$ och det för varje klartext $p \in \mathcal{P}$ och kryptotext $c \in \mathcal{C}$ finns en *unik* nyckel $k \in \mathcal{K}$ sådan att $e_k(p) = c$.

Perfekt sekretess

Definition (One-time Pad)

Låt n vara ett positivt heltal. Definiera att $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. För alla nycklar $k = (k_1, \dots, k_n) \in \mathcal{K}$, klartexter $p = (p_1, \dots, p_n) \in \mathcal{P}$ och kryptotexter $c = (c_1, \dots, c_n) \in \mathcal{C}$ definierar vi att

$$e_k(p) = (p_1 + k_1, \dots, p_n + k_n),$$

där alla operationer utförs i \mathbb{Z}_2 , och därefter definierar vi att
 $d_k = e_k$.

Nyckeln $k \in \mathcal{K}$ måste väljas slumpmässigt och får aldrig återanvändas.

Perfekt sekretess

- Perfekt sekretess är krångligt att uppnå.
- Använder "beräkningsmässigt säker" istället.

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- **Data Encryption Standard (DES)**
- Advanced Encryption Standard (AES)

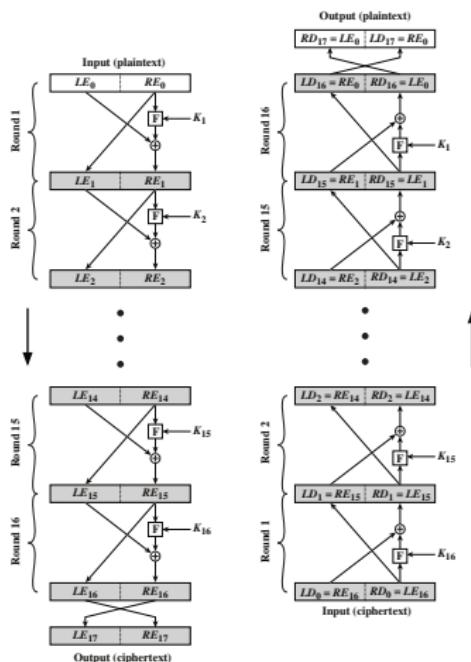
3 Pseudoslumptal och strömcipher

- Pseudoslumptal
- Strömcipher

4 Block Modes of Operation

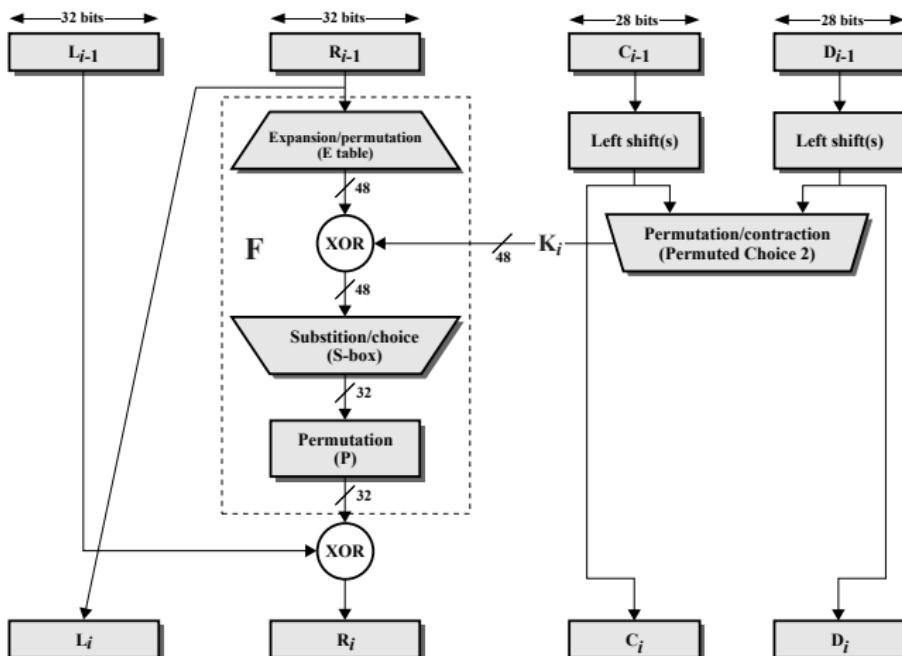
- Introduktion
- Några andra modes of operation

Data Encryption Standard (DES)



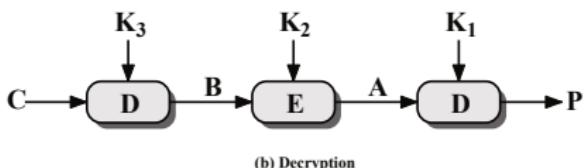
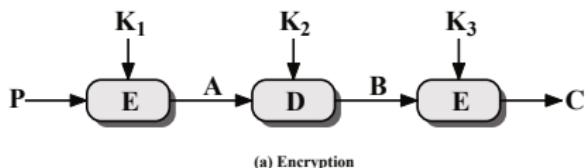
Figur : Feistelstruktur. Bild: [Sta11].

Data Encryption Standard (DES)



Figur : En runda i DES. Bild: [Sta11].

Data Encryption Standard (DES)



Figur : DES tillämpad i 3DES. Bild: [Sta11].

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

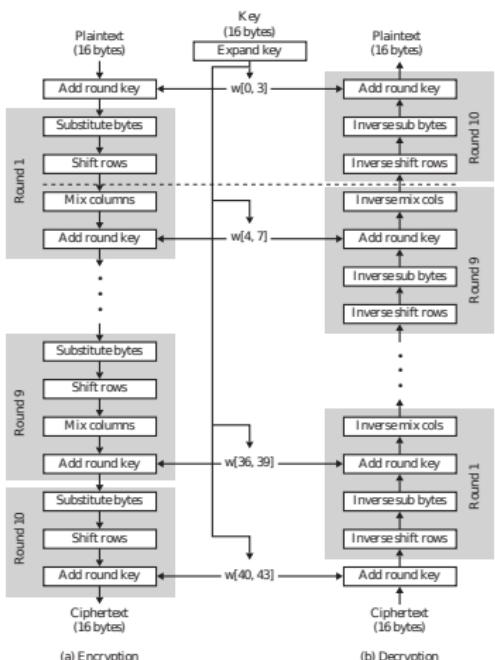
3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

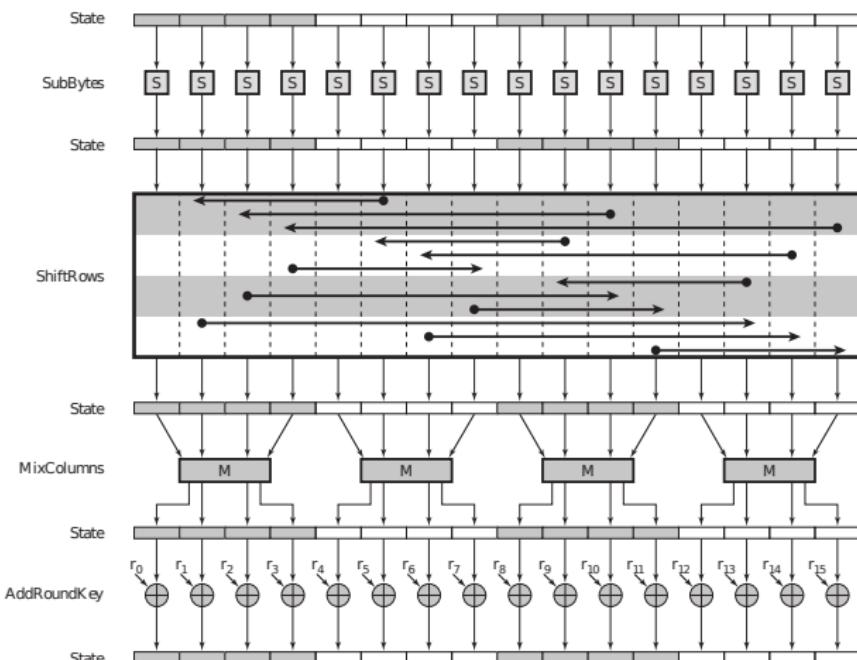
- Introduktion
- Några andra modes of operation

Advanced Encryption Standard (AES)



Figur : AES översikt. Bild: [Sta11].

Advanced Encryption Standard (AES)



Figur : En runda i AES. Bild: [Sta11].

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- **Pseudoslumptal**
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Pseudoslumptal

- Pseudorandom number generator.
- True random number generator.
- Pseudorandom function.



Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- **Strömchiffer**

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Strömchiffer

- Pseudorandom number generator som utgår från nyckeln.

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

3 Pseudoslumptal och strömchiffer

- Pseudoslumptal
- Strömchiffer

4 Block Modes of Operation

- **Introduktion**
- Några andra modes of operation

Introduktion

- Ett blockchiffer i standardutförande är inte särskilt säkert om vi vill kryptera mer än ett block med samma nyckel.
- För att åtgärda detta använder vi olika "modes of operation" för blockchiffer.

Introduktion

- Det mode of operation som vi hittills använt utan att benämna det som ett sådant är "electronic code-book mode" (ECB).
- Detta går som vi nämnt tidigare ut på att vi delar upp meddelandet enligt blockstorleken och krypterar del för del.

Översikt

1 Klassisk kryptografi

- Kryptosystem
- Substitutionschiffer
- Permutationschiffer
- Perfekt sekretess

2 Modern symmetrisk kryptering

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

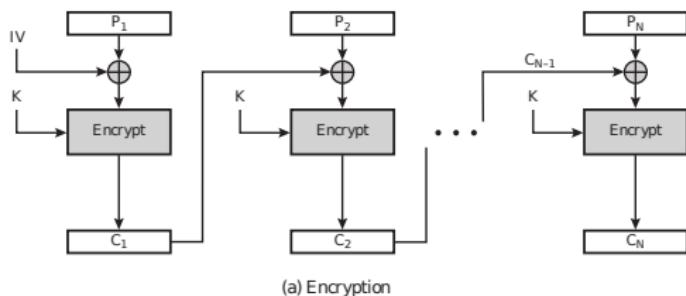
3 Pseudoslumptal och strömcipher

- Pseudoslumptal
- Strömcipher

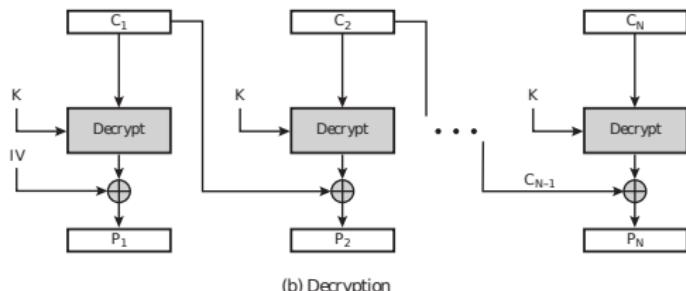
4 Block Modes of Operation

- Introduktion
- Några andra modes of operation

Några andra modes of operation



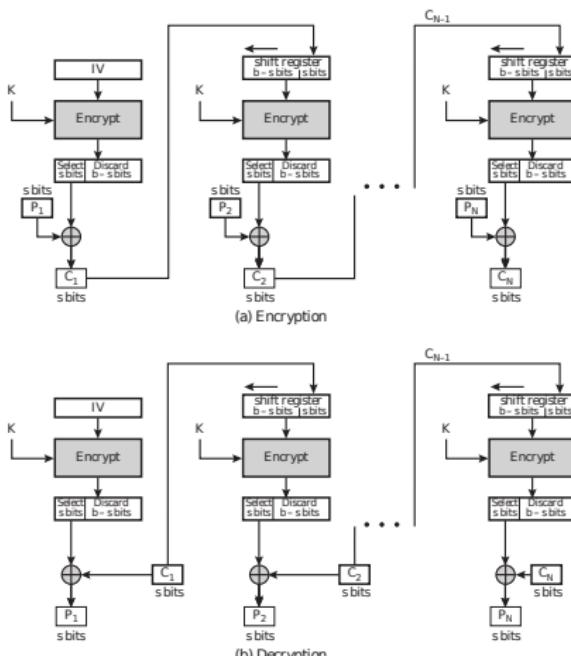
(a) Encryption



(b) Decryption

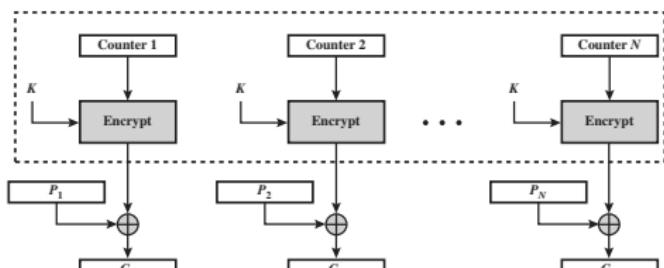
Figur : Cipher block chaining (CBC) mode. Bild: [Sta11].

Några andra modes of operation

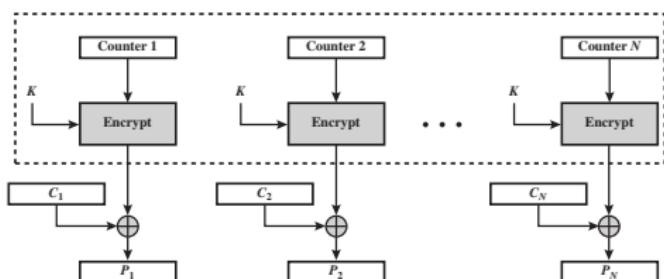


Figur : Cipher feedback (CFB) mode. Bild: [Sta11].

Några andra modes of operation



(a) Encryption



(b) Decryption

Figur : Counter (CTR) mode. Bild: [Sta11].

Referenser



Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems.* 2. utg. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL:
<http://www.cl.cam.ac.uk/~rja14/book.html>.



Daniel Bosk. "En introduktion till kryptografi". 2013.
URL: <http://ver.miun.se/courses/infosak/compendii/introcrypt.pdf>.



William Stallings. *Cryptography and network security : principles and practice.* 5. ed., International ed. Upper Saddle River: Prentice Hall, 2011. ISBN: 0-13-705632-X (pbk).



William Stallings. *Network security essentials : applications and standards.* 5. utg. International Edition.
Pearson Education, 2013. ISBN: 978-0-273-79336-6.