Symmetrisk kryptografi

Daniel Bosk[1]

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

symcrypt.tex 1989 2014-09-16 11:13:03Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

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

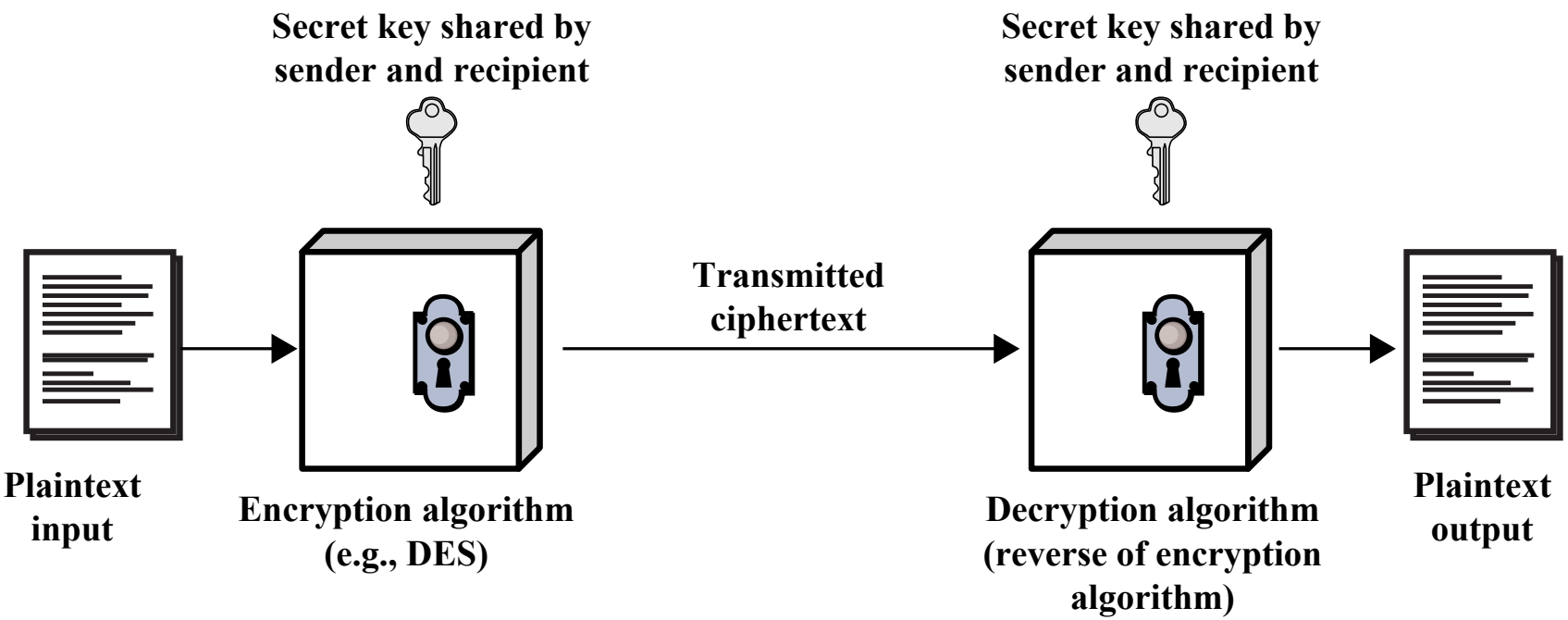
Litteratur

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* [And08].
You should then solve problems 2.1, 2.2, 2.12, 2.13 and 2.14 in [Sta13].

Kryptosystem

- Ordet kryptografi kommer från grekiskans κρυπτός (*kryptos*) och γράφος (*graphos*) [Oedb].
- Dessa betyder *gömd* eller *hemlig* [Oeda] respektive *skrift* [Oedc].
- 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 $e_k : \mathcal{P} \to \mathcal{C}$ och $d_k : \mathcal{C} \to \mathcal{P}$ är funktioner sådana att $d_k(e_k(p)) = p$ för alla klartexter $p \in \mathcal{P}$.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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

$$e_k(p) = (p + k) \bmod 29, \text{ och}$$
$$d_k(c) = (c - k) \bmod 29,$$

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

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 [Tea11].

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

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

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.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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

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

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

Substitutionschiffer
Sannolikhetsfördelningar

- Likformig sannolikhetsfördelning (uniform distribution).
- Oberoende.

Substitutionschiffer

α	A	B	C	D	E	F	G	H	I	J
$\Pr(\mathbf{Y} = \alpha)$	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
$\Pr(\mathbf{Y} = \alpha)$	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	
$\Pr(\mathbf{Y} = \alpha)$	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 meningen ”CPGPINKUJVGZVJCUPQUYGFKUJNGVVGTU”, angiven med tre decimalers noggrannhet.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Substitutionschiffer

Vigenèrechiffer

Definition (Vigenèrechiffer)

Låt n vara ett positivt heltal. Definiera att $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{29})^n$. För alla nycklar $k = (k_1, \ldots, k_n) \in \mathcal{K}$, klartexter $p = (p_1, \ldots, p_n) \in \mathcal{P}$ och kryptotexter $c = (c_1, \ldots, c_n) \in \mathcal{C}$ definierar vi att

$$e_k(p) = (p_1 + k_1, \ldots, p_n + k_n), \text{ och}$$
$$d_k(c) = (c_1 - k_1, \ldots, c_n - k_n),$$

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

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*.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Substitutionschiffer

Vigenèrechiffer

Exempel

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

```
skatten
ABCABCA
```

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

Substitutionschiffer

Vigenèrechiffer

Exempel

Ett Vigenèrechiffer 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.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

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 $\{1, \ldots, n\}$. För en permutation $\pi \in \mathcal{K}$ definierar vi

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

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

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

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

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 $p = (p_1, \ldots, p_n)$ vara vår klartext "en dag i juni", får vi att
$c = e_\pi(p) = (p_1, p_8, p_2, p_9, \ldots, p_7, p_{14})$ och således att c är vår kryptotext "EIN__JDUANGI_.".
Vi avkrypterar på samma sätt med hjälp av π^{-1}.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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* $e_k(p) = c$.

Mittuniversitetet
MID SWEDEN UNIVERSITY

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 $k = (k_1, \ldots, k_n) \in \mathcal{K}$, klartexter $p = (p_1, \ldots, p_n) \in \mathcal{P}$ och kryptotexter $c = (c_1, \ldots, c_n) \in \mathcal{C}$ definierar vi att

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

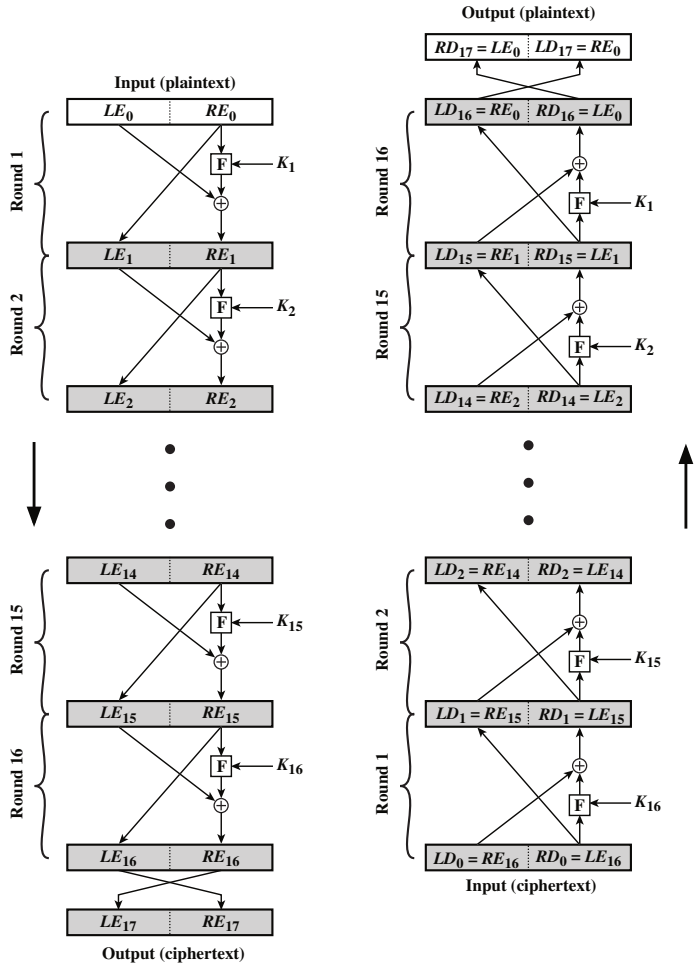
där alla operationer utförs i $\mathbb{Z}_2$, och därefter definierar vi att $d_k = e_k$.
Nyckeln $k \in \mathcal{K}$ måste väljas slumpmässigt och får aldrig återanvändas.

Mittuniversitetet
MID SWEDEN UNIVERSITY

Perfekt sekretess

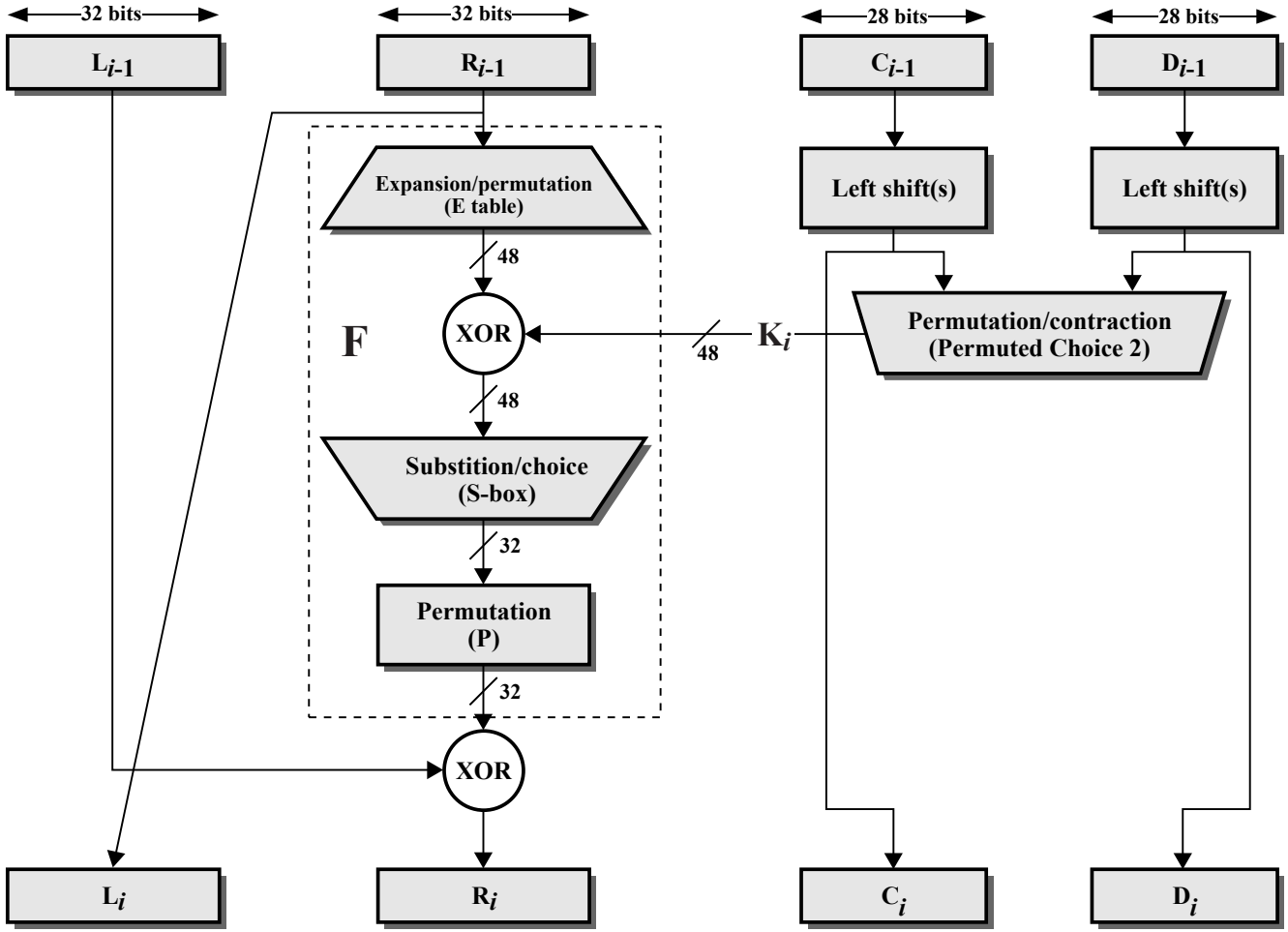
- Perfekt sekretess är krångligt att uppnå.
- Använder ”beräkningsmässigt säker” istället.

Data Encryption Standard (DES)



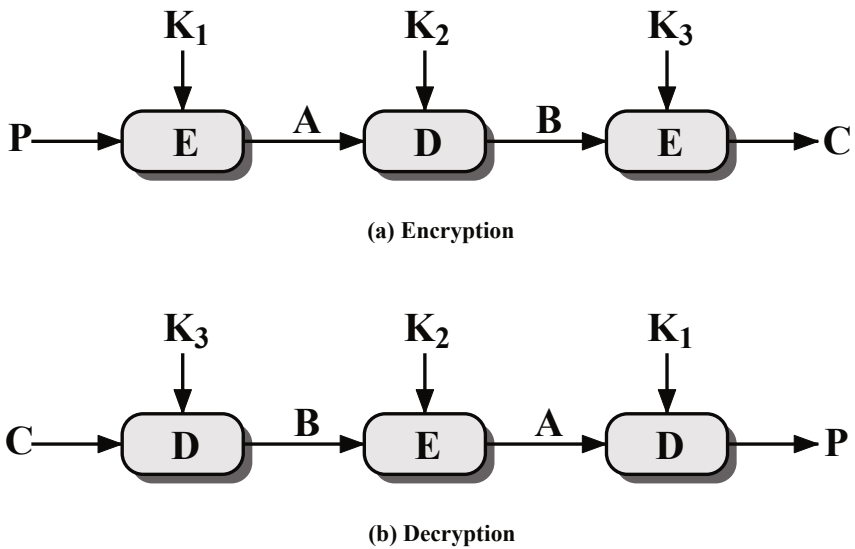
Figur: Feistelstruktur. Bild: [Sta11].

Data Encryption Standard (DES)



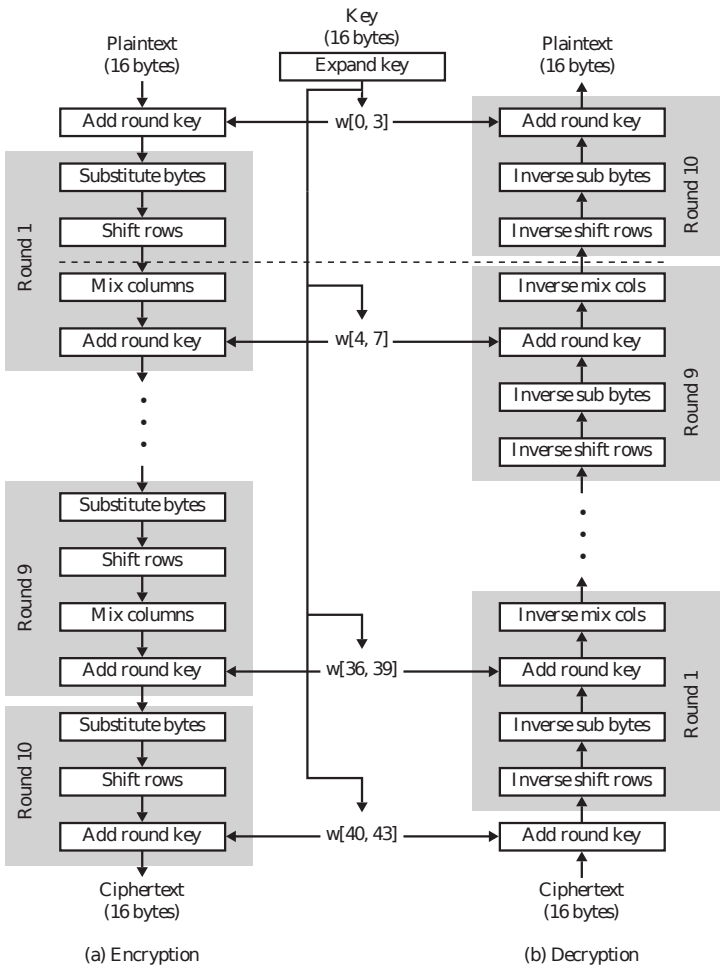
Figur: En runda i DES. Bild: [Sta11].

Data Encryption Standard (DES)



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

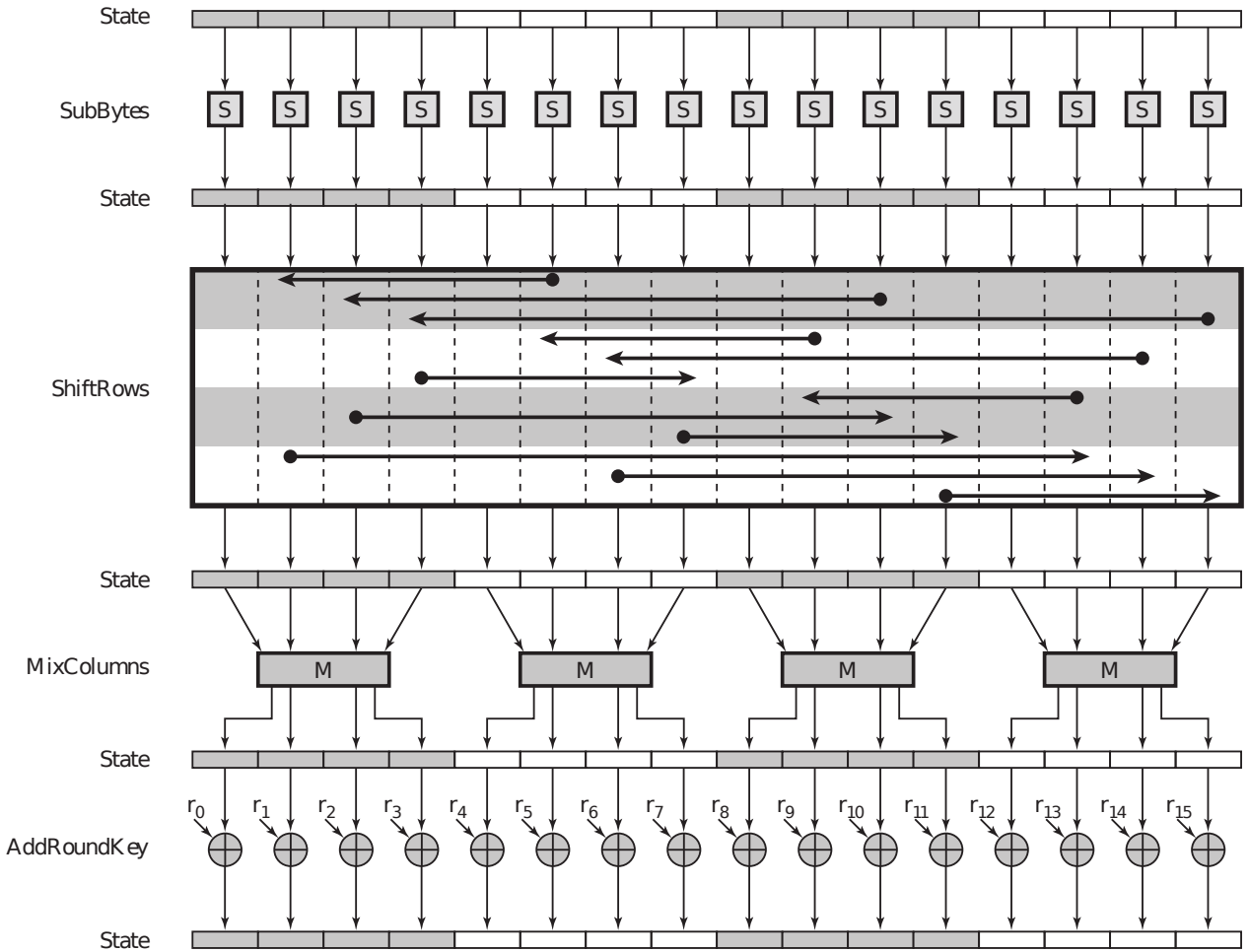
Advanced Encryption Standard (AES)



Figur: AES översikt. Bild: [Sta11].

Mittuniversitetet
MID SWEDEN UNIVERSITY

Advanced Encryption Standard (AES)



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

Mittuniversitetet
MID SWEDEN UNIVERSITY

Pseudoslumptal

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

Strömchiffer

- Pseudorandom number generator som utgår från nyckeln.

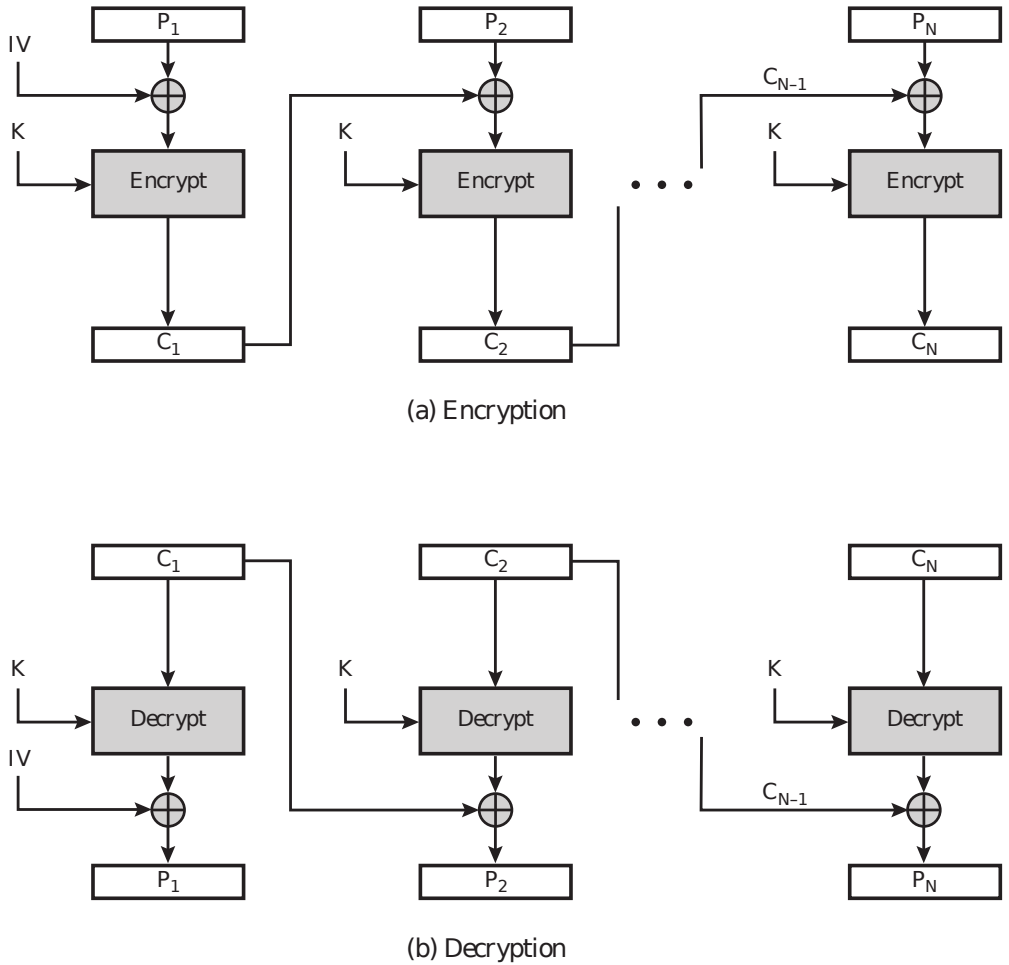
Introduktion

- 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

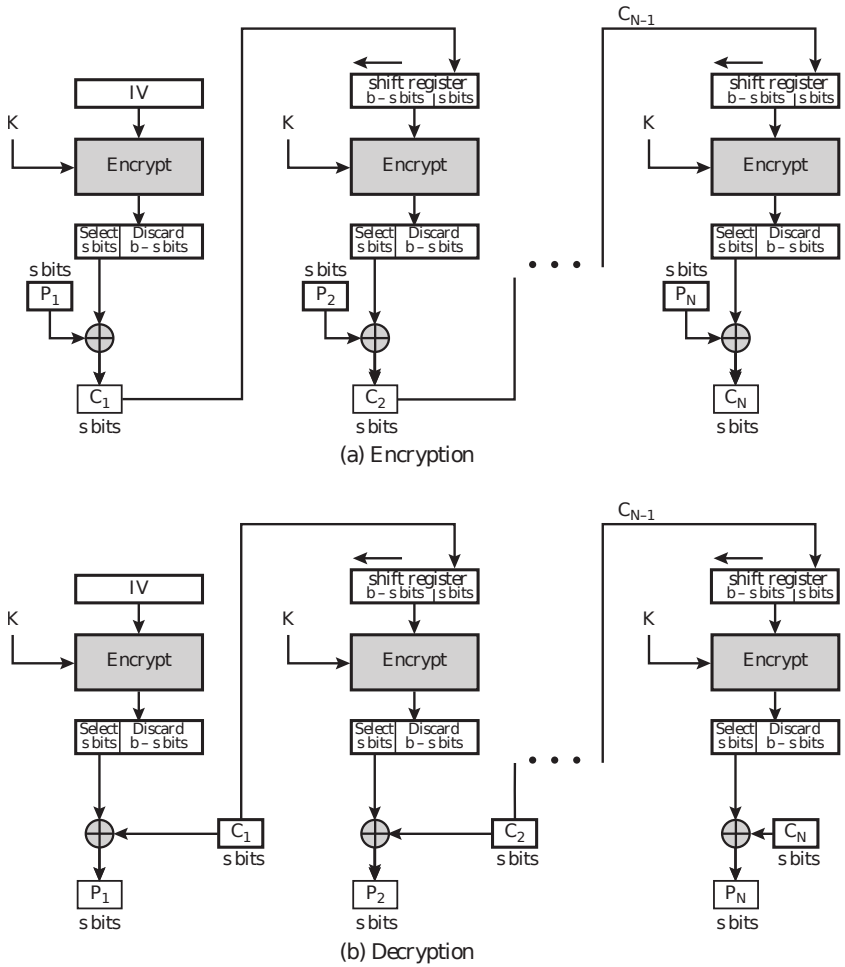
- Det mode of operation som vi hittills använt utan att benämna det som ett sådant är ”electronic code-book mode” (ECB).
- Detta går som vi nämnt tidigare ut på att vi delar upp meddelandet enligt blockstorleken och krypterar del för del.

Några andra modes of operation



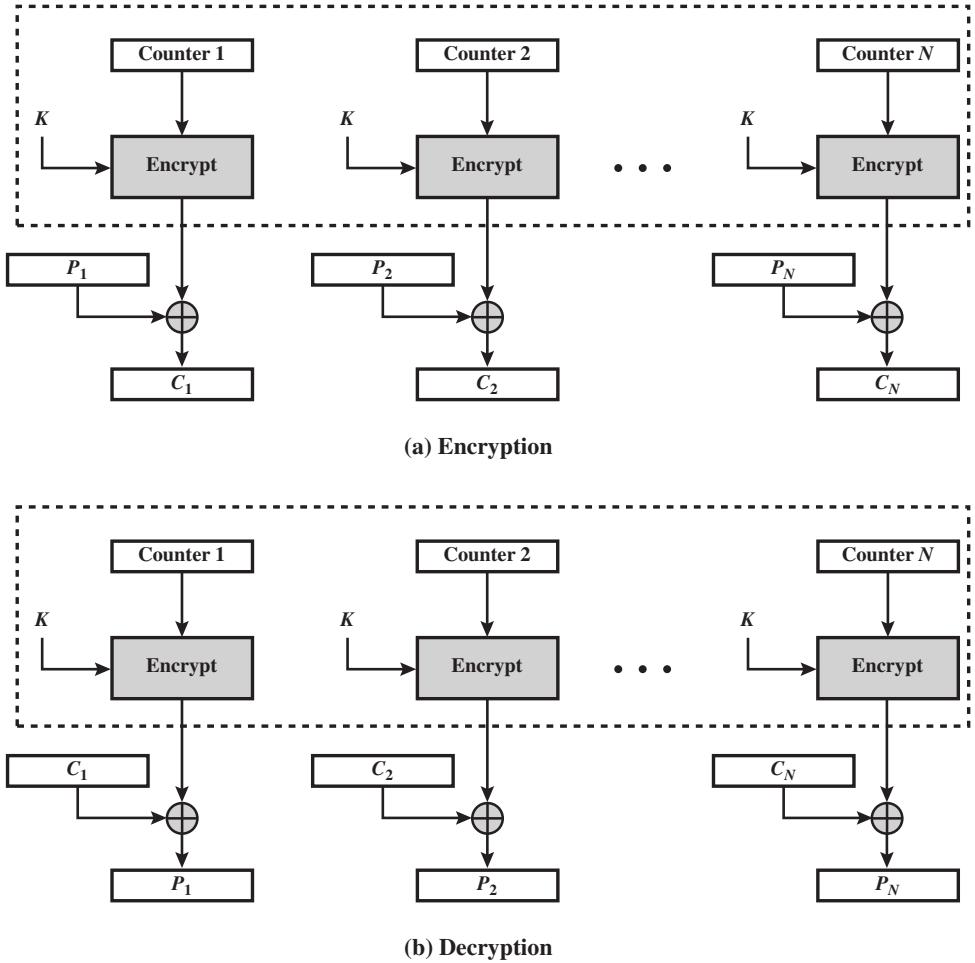
Figur: Cipher block chaining (CBC) mode. Bild: [Sta11].

Några andra modes of operation



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

Några andra modes of operation



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

Referenser

[And08] 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.

[Bos13] Daniel Bosk. "En introduktion till kryptografi". 2013. URL: http://ver.miun.se/courses/security/compendii/introcrypt.pdf.

[Oeda] "crypto-, comb. form". I: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, mars 2013. URL: http://www.oed.com/view/Entry/45363.

[Oedb] "cryptography, n." I: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, mars 2013. URL: http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography&.

[Oedc] "graphy, comb. form". I: *OED Online*. Hämtad den 5