


Översikt av kryptografiska mekanismer

Daniel Bosk¹

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

crypto.tex 1009 2013-05-02 22:14:41Z 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 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

Litteratur

Föreläsningen går väsentligen igenom [Bos13] och kapitel 5 "Cryptography" i [And08].

Översikt

- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

Översikt

- 1 Klassisk kryptografi
 - **Kryptosystem**
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess

- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation

- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

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 $p \in \mathcal{P}$.

Översikt

- 1 Klassisk kryptografi
 - Kryptosystem
 - **Substitutionschiffer**
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

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.

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.

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

Substitutionschiffer

$\Pr(Y = \alpha)$	A	B	C	D	E	F	G	H	I	J
	0.000	0.000	0.063	0.000	0.000	0.031	0.156	0.000	0.031	0.094
$\Pr(Y = \alpha)$	K	L	M	N	O	P	Q	R	S	T
	0.064	0.000	0.000	0.063	0.000	0.094	0.031	0.000	0.000	0.031
$\Pr(Y = \alpha)$	U	V	W	X	Y	Z	Å	Ä	Ö	
	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 "CPGPINKUJVGZVJJCUPQUYGFKUJNGVVGTU", angiven med tre decimalers noggrannhet.

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 $k = (k_1, \dots, k_n) \in \mathcal{K}$, 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

Vigenèrechiffer

Exempel

Om vi vill kryptera ordet *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.

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 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

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 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

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.

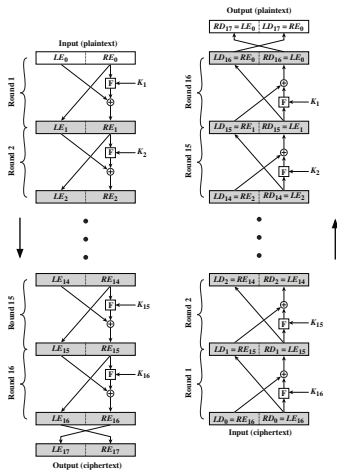
Översikt

- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

Översikt

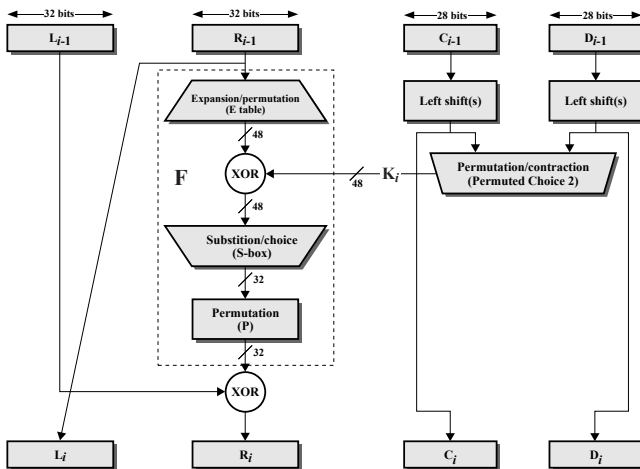
- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - **Data Encryption Standard (DES)**
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

Data Encryption Standard (DES)



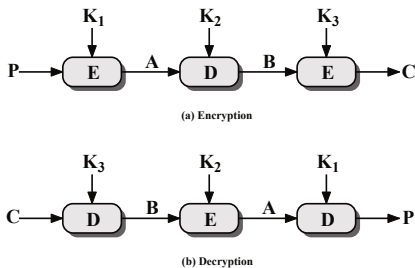
Figur : Feistelstruktur. Bild: [Sta11].

Data Encryption Standard (DES)



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

Data Encryption Standard (DES)

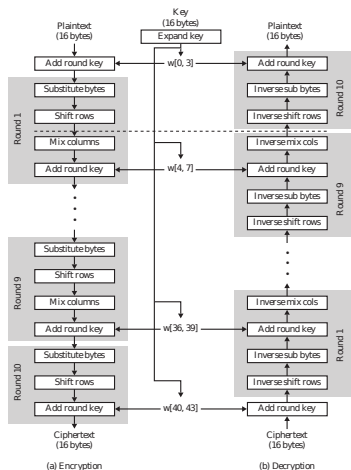


Figur : DES tillämpad i 3DES. Bild: [Sta11].

Översikt

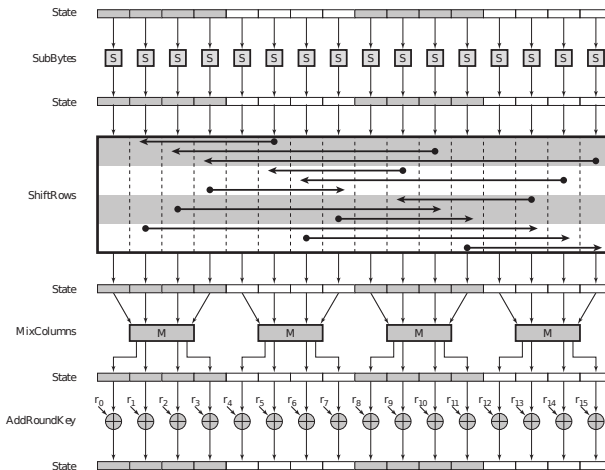
- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - **Advanced Encryption Standard (AES)**
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

Advanced Encryption Standard (AES)



Figur : AES översikt. Bild: [Sta11].

Advanced Encryption Standard (AES)

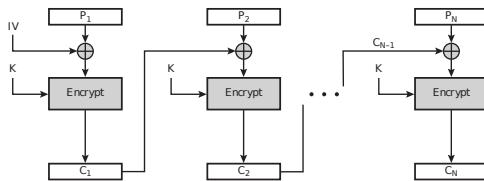


Figur : En runda i AES. Bild: [Sta11].

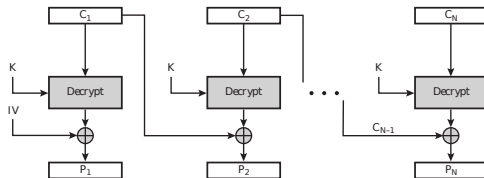
Översikt

- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - **Block Modes of Operation**
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

Block Modes of Operation



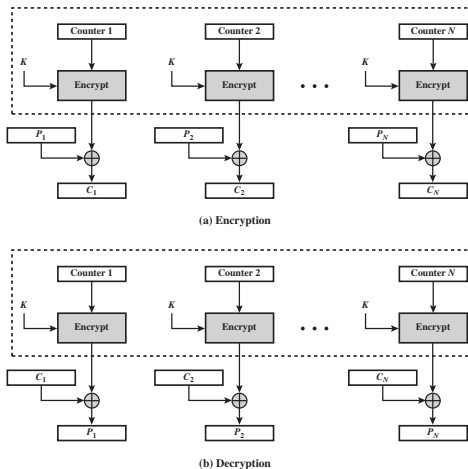
(a) Encryption



(b) Decryption

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

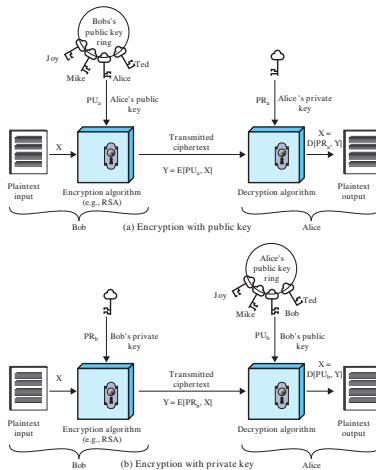
Block Modes of Operation



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

Översikt

- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem



Figur : Översikt av asymmetrisk kryptering. Bild: [Sta11].

Översikt

- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - **Talteori**
 - Kryptosystem

Talteori

Sats (Fermat-Eulers sats)

Om n och a är heltal sådana att $\gcd(n, a) = 1$, då gäller att $a^{\phi(n)} \equiv 1 \pmod{n}$.

Översikt

- 1 Klassisk kryptografi
 - Kryptosystem
 - Substitutionschiffer
 - Permutationschiffer
 - Perfekt sekretess
- 2 Symmetrisk kryptering
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
 - Block Modes of Operation
- 3 Asymmetrisk kryptering
 - Talteori
 - Kryptosystem

Kryptosystem

Rivest, Shamir, Adleman (RSA)

Definition

Låt $n = pq$, där p och q är primtal. Låt $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ och

$$\mathcal{K} = \{(n, p, q, e, d) : ed \equiv 1 \pmod{\phi(n)}\}.$$

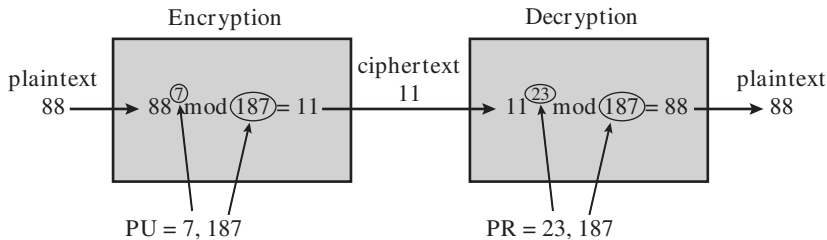
För $k = (n, p, q, e, d)$ definiera

$$e_k(p) = p^e \pmod{n} \text{ och}$$

$$d_k(c) = c^d \pmod{n},$$

där $p \in \mathcal{P}$ och $c \in \mathcal{C}$. Tupeln (n, e) utgör den *publika nyckeln* och (p, q, d) den *privata nyckeln*.

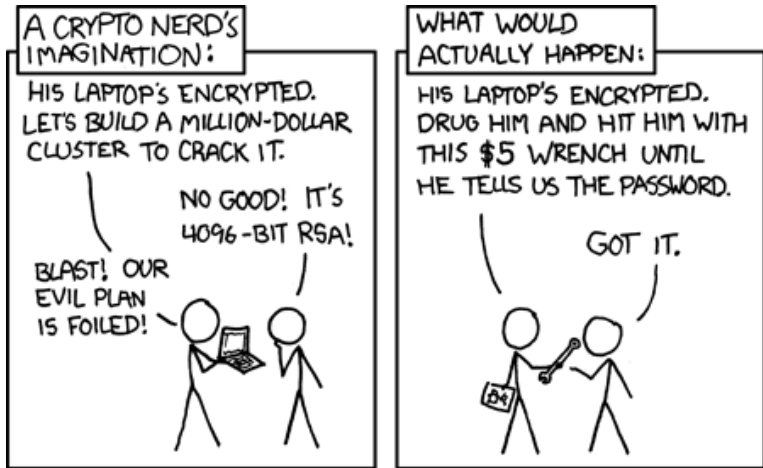
Kryptosystem



Figur : Ett exempel på kryptering med RSA. Bild: [Sta11].

Kryptosystem

Men glöm ej ...



Figur : En serieruta som illustrerar vikten av den sociala aspekten på säkerhet. Bild: [xkc].

Referenser

- [And08] Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems*. Wiley, Indianapolis, IN, 2 utgåvan, 2008.
- [Bos13] Daniel Bosk. Introduktion till några klassiska chiffer. 2013.
- [OED13a] crypto-, comb. form. I: *OED Online*. Oxford University Press, mar 2013. Hämtad den 5 april 2013.
- [OED13b] cryptography, n. I: *OED Online*. Oxford University Press, mar 2013. Hämtad den 5 april 2013.
- [OED13c] graphy-, comb. form. I: *OED Online*. Oxford University Press, mar 2013. Hämtad den 5 april 2013.
- [Sta11] William Stallings. *Cryptography and network security : principles and practice*. Prentice Hall, Upper Saddle River, 5. ed., international ed. utgåvan, 2011.
- [Tea11] Team Register. BA jihadist relied on jesus-era encryption, mar 2011.
- [xkc] xkcd. Security.