

Szyfrowanie danych w SZBD

dr inż. Maciej Nikodem

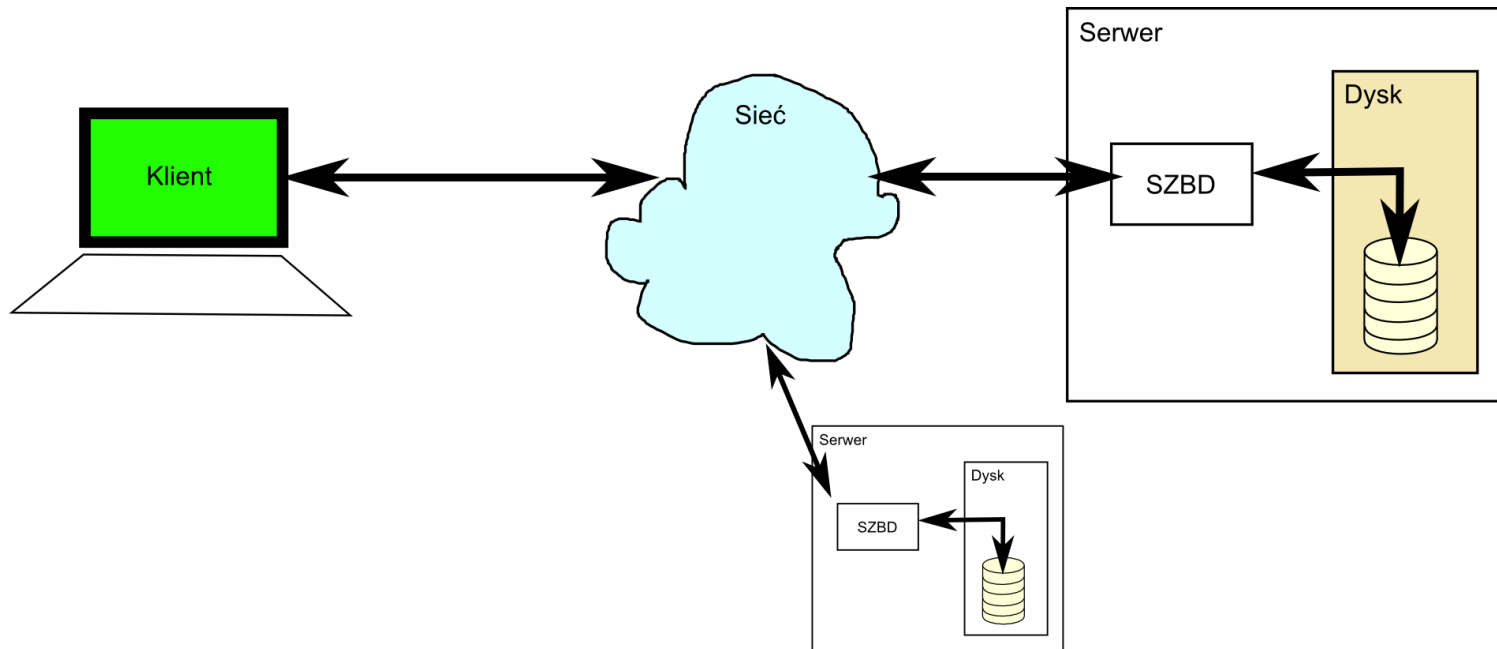
Instytut Informatyki, Automatyki i Robotyki

maciej.nikodem@pwr.wroc.pl

Czy potrzebujemy szyfrowania w SZBD?

- prawo,
- kontrola dostępu,
- ochrona przed:
 - administratorem,
 - właścicielem serwerów
- duże ilości danych,
- przesyłanie w sieciach,
- nośniki
- ...

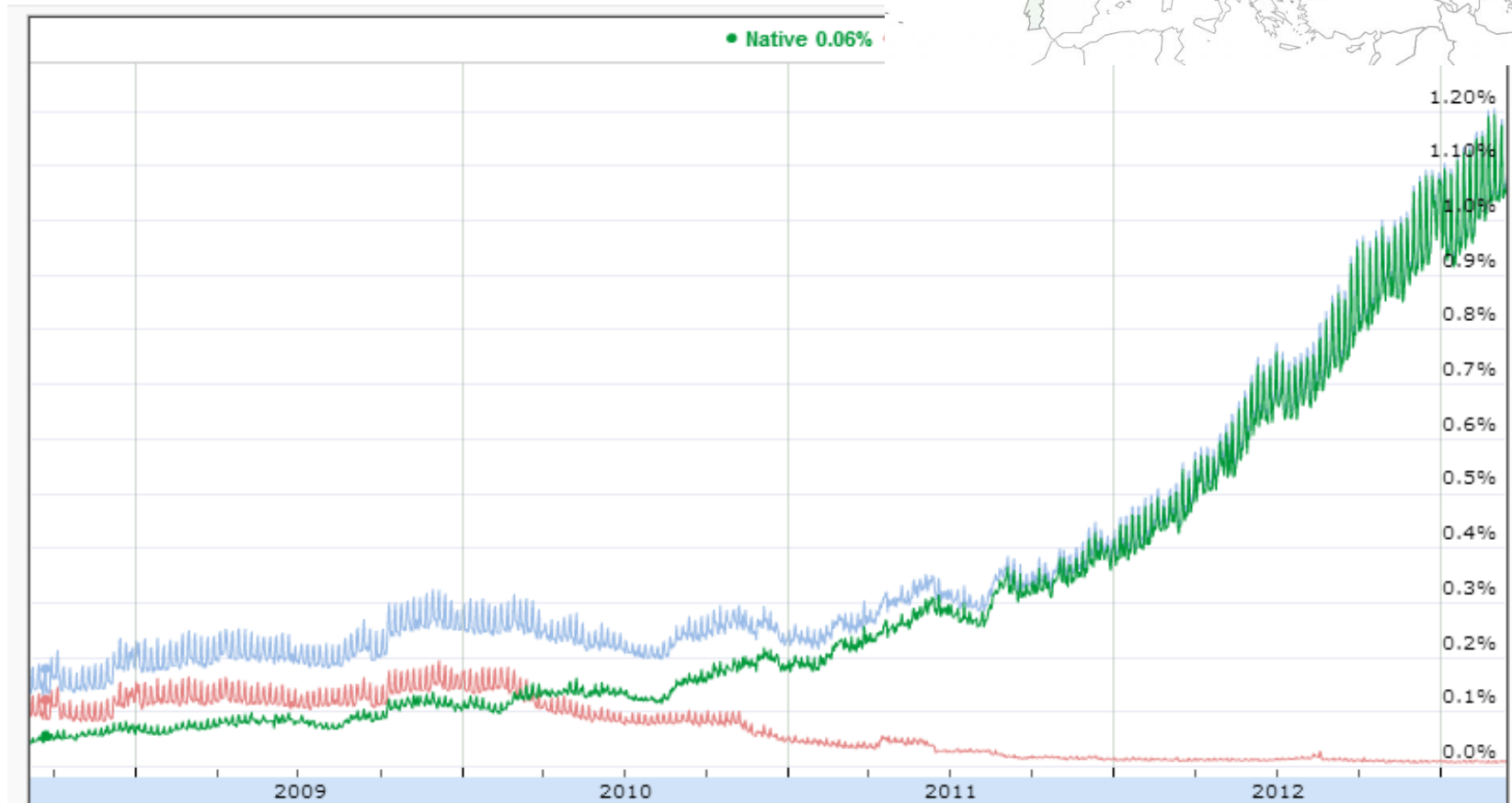
Sieć i aplikacje



- nośniki – baza, logi, kopie zapasowe,
- pamięć – przetwarzane dane,
- przesyłanie – logowanie, zapytania, wyniki,
- operacje SZBD

Bezpieczeństwo komunikacji

- SSL/TSL,
- IP6



Konsekwencje

- domyślna ochrona
 - poprawność?
 - poufność?
 - autentyczność?

Miejsca zagrożeń:

- przechowywanie na nośnikach,
- przesyłanie w sieciach teleinformatycznych
- przechowywanie w pamięci

Przykład 1



PORTAL DLA LUDZI Z KLASĄ

[Edytuj profil](#) · [Pomoc](#) · [Zaloguj](#)

Start ▾ & Profil

nasza-klasa.pl
PORTAL DLA LUDZI Z KLASĄ

Taniej niż w sklepie
Przed świętami

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.15.202	195.93.178.6	TCP	51728 > http [SYN] Seq=0 Len=0 MSS=1260 WS=2
2	0.017224	195.93.178.6	192.168.15.202	TCP	http > 51728 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
3	0.017340	192.168.15.202	195.93.178.6	TCP	51728 > http [ACK] Seq=1 Ack=1 win=17640 Len=0
4	0.043480	192.168.15.202	195.93.178.6	HTTP	POST /login HTTP/1.1 (application/x-www-form-urlencoded)
5	0.060445	195.93.178.6	192.168.15.202	TCP	http > 51728 [ACK] Seq=1 Ack=837 win=6688 Len=0
6	0.085173	195.93.178.6	192.168.15.202	TCP	[TCP segment of a reassembled PDU]

▢ Frame 4 (890 bytes on wire, 890 bytes captured)

▢ Ethernet II, Src: GemtekTe_1f:e7:d1 (00:1a:73:1f:e7:d1), Dst: Cisco-Li_33:ac:32 (00:18:39:33:ac:32)

▢ Internet Protocol, Src: 192.168.15.202 (192.168.15.202), Dst: 195.93.178.6 (195.93.178.6)

▢ Transmission Control Protocol, Src Port: 51728 (51728), Dst Port: http (80), Seq: 1, Ack: 1, Len: 836

Source port: 51728 (51728)

Destination port: http (80)

Zaloguj się

Login lub e-mail:

Hasło:

☐ pamiętaj mnie

Nie masz jeszcze konta z klasą? [Zaloguj](#)

Nie pamiętasz hasła?
Nie dotarł do Ciebie e-mail z linkiem aktywacji?
[Zaloguj się używając protokołu SSL](#)

Wyszukiwanie

<pre> 01e0 6e 61 73 7a 61 2d 6b 6c 61 73 61 2e 70 6c 2f 0d 01f0 0a 43 6f 6f 6b 69 65 3a 20 6e 6b 5f 73 65 73 73 0200 69 6f 6e 3d 34 52 37 59 78 49 25 32 43 67 38 59 0210 78 55 4a 56 49 45 44 67 30 37 5a 75 6d 65 36 42 0220 35 3b 20 6a 73 5f 65 6e 61 62 6c 65 64 3d 31 3b 0230 20 6e 6b 5f 77 69 6e 64 6f 77 3d 66 6f 63 75 73 0240 65 64 3b 20 6d 3d 6e 3b 20 5f 5f 75 74 6d 61 3d 0250 31 37 34 34 32 30 38 36 2e 32 37 34 35 33 39 39 0260 35 30 38 37 32 30 32 30 37 30 30 30 2e 31 32 34 0270 32 34 36 34 37 38 34 2e 31 32 34 32 34 36 34 37 0280 38 34 2e 31 32 34 32 34 36 34 37 38 34 2e 31 3b 0290 20 5f 5f 75 74 6d 62 3d 31 37 34 34 32 30 38 36 02a0 2e 31 2e 31 30 2e 31 32 34 32 34 36 34 37 38 34 02b0 3b 20 5f 5f 75 74 6d 63 3d 31 37 34 34 32 30 38 02c0 36 3b 20 5f 5f 75 74 6d 7a 3d 31 37 34 34 32 30 02d0 38 36 2e 31 32 34 32 34 36 34 37 38 34 2e 31 2e 02e0 31 2e 75 74 6d 63 73 72 3d 28 64 69 72 65 63 74 02f0 29 7c 75 74 6d 63 63 6e 3d 28 64 69 72 65 63 74 0300 29 7c 75 74 6d 63 6d 64 3d 28 6e 6f 6e 65 29 0d 0310 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 0320 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 0330 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0340 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 0350 3a 20 33 34 0d 0a 0d 0a 6c 6f 67 69 6e 3d 6d 6e 0360 69 6b 6f 64 65 6d 26 70 61 73 73 77 6f 72 64 3d 0370 74 61 6a 6e 65 68 61 73 6c 6f </pre>	<pre> nasza-klasa.pl/. .Cookie: nk_sess ion=4R7Y xI%2Cg8Y xUJVIEDg 07zume6B 5; js_enabled=1; nk_window=focus ed; m=n; __utma= 17442086.2745399 50872020 7000.124 2464784. 12424647 84.12424 64784.1; __utmb= 17442086 .1.10.12 42464784 ; __utmc=1744208 6; __utmz=174420 86.12424 64784.1. 1.utmcsr=(direct) utmccn=(direct) utmcmd=(none). .Content-Type: a pplicati on/x-www -form-ur lencoded ..Content-Length : 34.... login=mn ikodem& password= tajnehaslo </pre>
--	--

6

Przykład 2 - MySQL

3	0.029843	192.168.15.202	156.17.42.79	TCP	56404 > 3306 [ACK] Seq=1 Ack=1 win=17640 Len=0
4	0.060288	156.17.42.79	192.168.15.202	MySQL	Server Greeting proto=10 version=5.1.31-log
5	0.060643	192.168.15.202	156.17.42.79	MySQL	Login Request user=mnikodem
6	0.090039	156.17.42.79	192.168.15.202	TCP	3306 > 56404 [ACK] Seq=61 Ack=67 win=5840 Len=0
7	0.090841	156.17.42.79	192.168.15.202	MySQL	Response OK
8	0.091215	192.168.15.202	156.17.42.79	MySQL	Request Query

Salt: 9!724Psr

- ⊕ Server Capabilities: 0xF7FF
Charset: latin1 COLLATE latin1_swedish_ci (8)
- ⊕ Server Status: 0x0002
Unused:

Salt: cyv%SQ}Cr7x8

```

0000 00 1a 73 1f e7 d1 00 18 39 33 ac 32 08 00 45 00 ..s.... 93.2..E.
0010 00 64 a3 d9 00 00 2b 06 54 e8 9c 11 2a 4f c0 a8 .d....+. T...*O..
0020 0f ca 0c ea dc 54 f4 9b 98 2e b4 e7 a5 73 50 18 .....T.. ....sP.
0030 16 d0 f7 db 00 00 38 00 00 00 0a 35 2e 31 2e 33 .....8. ...5.1.3
0040 31 2d 6c 6f 67 00 e1 03 00 00 39 21 37 32 34 50 1-log... ..9!724P
0050 73 72 00 ff f7 08 02 00 00 00 00 00 00 00 00 sr.....
0060 00 00 00 00 00 63 79 56 25 53 51 7d 43 72 37 58 .....cyv %SQ}Cr7X
0070 38 00 8.

```

3	0.029843	192.168.15.202	156.17.42.79	TCP	56404 > 3306 [ACK] Seq=1 Ack=1 win=17640 Len=0
4	0.060288	156.17.42.79	192.168.15.202	MySQL	Server Greeting proto=10 version=5.1.31-log
5	0.060643	192.168.15.202	156.17.42.79	MySQL	Login Request user=mnikodem
6	0.090039	156.17.42.79	192.168.15.202	TCP	3306 > 56404 [ACK] Seq=61 Ack=67 win=5840 Len=0
7	0.090841	156.17.42.79	192.168.15.202	MySQL	Response OK
8	0.091215	192.168.15.202	156.17.42.79	MySQL	Request Query

- ⊕ Client Capabilities: 0xA285
- ⊕ Extended Client Capabilities: 0x0002
MAX Packet: 1073741824
Charset: utf8 COLLATE utf8_general_ci (33)
Username: mnikodem

Password: \026\246\003\2036\t\021\022\032xg\005 \265|xant#

```

0000 00 18 39 33 ac 32 00 1a 73 1f e7 d1 08 00 45 00 ..93.2.. s.....E.
0010 00 6a 10 73 40 00 80 06 53 48 c0 a8 0f ca 9c 11 .j.s@... SH.....
0020 2a 4f dc 54 0c ea b4 e7 a5 73 f4 9b 98 6a 50 18 *O.T.... .s...jP.
0030 11 2b 4e e7 00 00 3e 00 00 01 85 a2 02 00 00 00 .+N...>. ....
0040 00 40 21 00 00 00 00 00 00 00 00 00 00 00 00 .@!.....
0050 00 00 00 00 00 00 00 00 00 00 6d 6e 69 6b 6f 64 ..... ..mnikod
0060 65 6d 00 14 16 a6 03 83 36 09 11 12 1a 78 67 05 em..... 6....xg.
0070 20 b5 7c 58 61 6e 74 23 .|xant#

```


Przykład 3 - MySQL

No. -	Time	Source	Destination	Protocol	Info
9	3.037038	156.17.42.79	192.168.15.202	MySQL	Response
10	3.038325	192.168.15.202	156.17.42.79	MySQL	Request Query
11	3.068932	156.17.42.79	192.168.15.202	MySQL	Response
12	3.069761	192.168.15.202	156.17.42.79	MySQL	Request Query
13	3.101945	156.17.42.79	192.168.15.202	MySQL	Response
14	3.102177	156.17.42.79	192.168.15.202	MySQL	Response
15	3.102218	192.168.15.202	156.17.42.79	TCP	58282 > 3306 [ACK
16	5.030856	192.168.15.202	156.17.42.79	MySQL	Request Ping

Internet Protocol, Src: 192.168.15.202 (192.168.15.202), Dst: 156.17.42.79 (156.17.42.79)

Transmission Control Protocol, Src Port: 58282 (58282), Dst Port: 3306 (3306), Seq: 94,

MySQL Protocol

Packet Length: 23

Packet Number: 0

Command

No. -	Time	Source	Destination	Protocol	Info
9	3.037038	156.17.42.79	192.168.15.202	MySQL	Response
10	3.038325	192.168.15.202	156.17.42.79	MySQL	Request Query
11	3.068932	156.17.42.79	192.168.15.202	MySQL	Response
12	3.069761	192.168.15.202	156.17.42.79	MySQL	Request Query
13	3.101945	156.17.42.79	192.168.15.202	MySQL	Response
14	3.102177	156.17.42.79	192.168.15.202	MySQL	Response
15	3.102218	192.168.15.202	156.17.42.79	TCP	58282 > 3306 [ACK]
16	5.030856	192.168.15.202	156.17.42.79	MySQL	Request Ping

```

0000  00 18 39 33 ac 32 00 1a 73 1f e7 d1 08 00 45 00  ..93.2.. s.....E.
0010  00 43 52 5b 40 00 80 06 11 87 c0 a8 0f ca 9c 11  .CR[@.....
0020  2a 4f e3 aa 0c ea 92 8c 14 84 3c 11 1b 5c 50 18  *O..... <...P.
0030  11 3a 8f 1d 00 00 17 00 00 00 03 53 45 4c 45 43  ..... ..SELEC
0040  54 20 2a 20 46 52 4f 4d 20 73 74 75 64 65 6e 63  T * FROM studenc
0050  69  i

```

No. -	Time	Source	Destination	Protocol	Info
9	3.037038	156.17.42.79	192.168.15.202	MySQL	Response
10	3.038325	192.168.15.202	156.17.42.79	MySQL	Request Query
11	3.068932	156.17.42.79	192.168.15.202	MySQL	Response
12	3.069761	192.168.15.202	156.17.42.79	MySQL	Request Query
13	3.101945	156.17.42.79	192.168.15.202	MySQL	Response
14	3.102177	156.17.42.79	192.168.15.202	MySQL	Response
15	3.102218	192.168.15.202	156.17.42.79	TCP	58282 > 3306 [ACK]
16	5.030856	192.168.15.202	156.17.42.79	MySQL	Request Ping

No. -	Time	Source	Destination	Protocol	Info
9	3.037038	156.17.42.79	192.168.15.202	MySQL	Response
10	3.038325	192.168.15.202	156.17.42.79	MySQL	Request Query
11	3.068932	156.17.42.79	192.168.15.202	MySQL	Response
12	3.069761	192.168.15.202	156.17.42.79	MySQL	Request Query
13	3.101945	156.17.42.79	192.168.15.202	MySQL	Response
14	3.102177	156.17.42.79	192.168.15.202	MySQL	Response
15	3.102218	192.168.15.202	156.17.42.79	TCP	58282 > 3306 [ACK]
16	5.030856	192.168.15.202	156.17.42.79	MySQL	Request Ping

No. -	Time	Source	Destination	Protocol	Info
9	3.037038	156.17.42.79	192.168.15.202	MySQL	Response
10	3.038325	192.168.15.202	156.17.42.79	MySQL	Request Query
11	3.068932	156.17.42.79	192.168.15.202	MySQL	Response
12	3.069761	192.168.15.202	156.17.42.79	MySQL	Request Query
13	3.101945	156.17.42.79	192.168.15.202	MySQL	Response
14	3.102177	156.17.42.79	192.168.15.202	MySQL	Response
15	3.102218	192.168.15.202	156.17.42.79	TCP	58282 > 3306 [ACK]
16	5.030856	192.168.15.202	156.17.42.79	MySQL	Request Ping

Przykład 4 - MsSQL

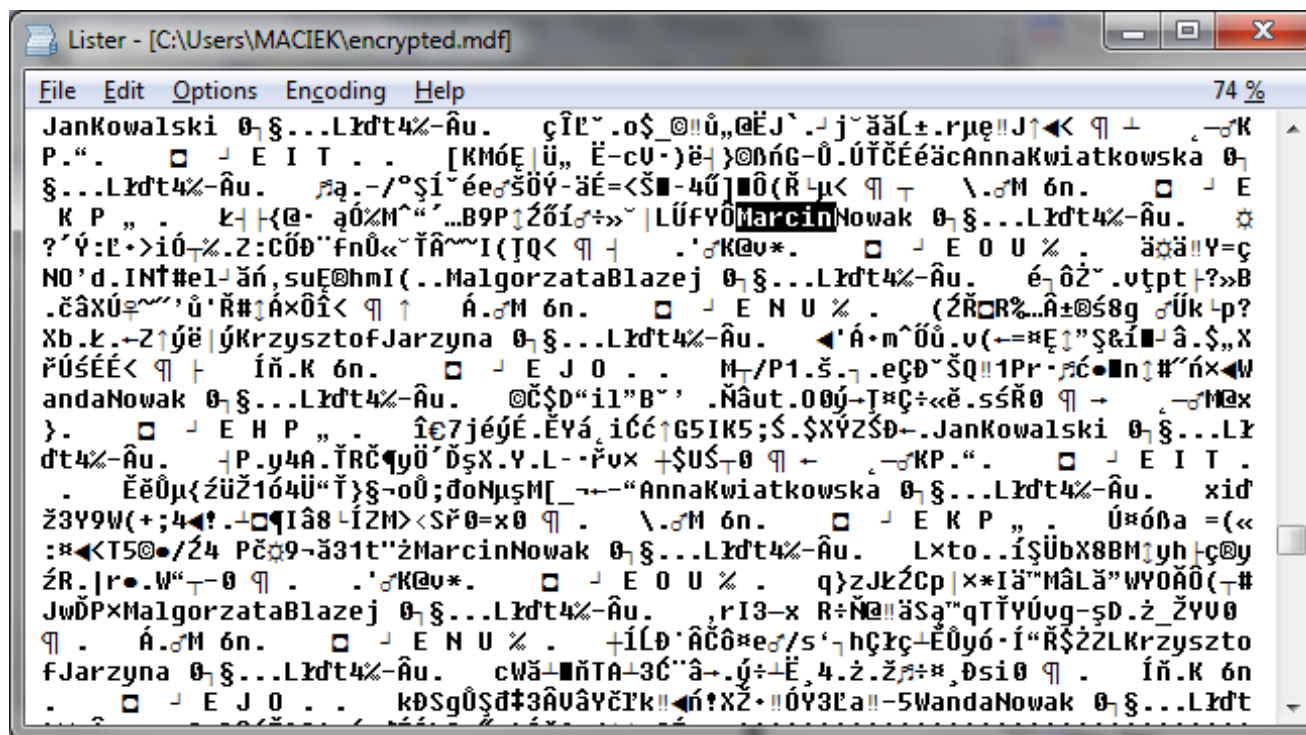
[illegible][illegible]

Lister - [C:\Users\MACIEK\encrypted.mdf]

File Edit Options Encoding Help

JanKowalski 0§...Łłđt4%-Āu. ċİE~.o\$
P.“. □ ▽ E I T . . [KMóEü] Ē-cv
S...Łłđt4%-Āu. řā.-°ŝí'ēešōŷ-āÉ=◁Š
K P . . k┘|@- a0M“~..B9P`žōī◊+» |
?´Y:ē┐ıō◊.Z:CÜÖ`řñú◊ İÄ~İ(IQ◊ İ
MO'd.INT#elı šñ,suf@hmi(..MalgorzataBlaz
.čāXū◊`ü`Řñ;Áxōİ◊ ◊ ↑ Á.M 6n.
Xb.┘-┘ZjğŸKrzyśtofJarzyna 0§...Łłđt
RÚŚÉÉ◊ ◊ ↑ İñ.K 6n. □ ▽ E J O .
andaNowak 0§...Łłđt4%-Āu. @šĐP“il”B
}. □ ▽ E H P . . İE7jéğĖ.EVá icé
đt4%-Āu. ┘P.y4A.İRČqyö`D\$X.Y.L-řux-
Ĕëöµ┘Zúİ2ı6ăU~İ}§s-o0;đonµşM[---“A
ż3Y9W(+;4đ;-□İA8-İZM)◊ŞF0=x0 ◊ . \
:◊◊◊T50◊/Z4 Pēō9-ā31t”zMarcinNowak 0§
ZR.|rø.W~-T0 ◊ . .'K@v*. □ ▽ E I
JwđP×MalgorzataBlazej 0§...Łłđt4%-Āu.
◊ . Á.M 6n. □ ▽ E N U . . +İİ
fJarzyna 0§...Łłđt4%-Āu. cWā-■ñTA-3
... □ ▽ E J O . . kōSgōšđ3āŪāVçIK

Przykład 4 - MsSQL



The screenshot shows a Notepad window titled "Lister - [C:\Users\MACIEK\encrypted.mdf]". The window contains a list of names, each preceded by a tab character and a string of characters that appear to be a file path or identifier. The names are: JanKowalski, AnnaKwiatkowska, MarcinNowak, MalgorzataBlazej, KrzysztofJarzyna, WandaNowak, and fJarzyna. The text is displayed in a monospaced font, and the window has a standard Windows interface with a menu bar and a status bar.

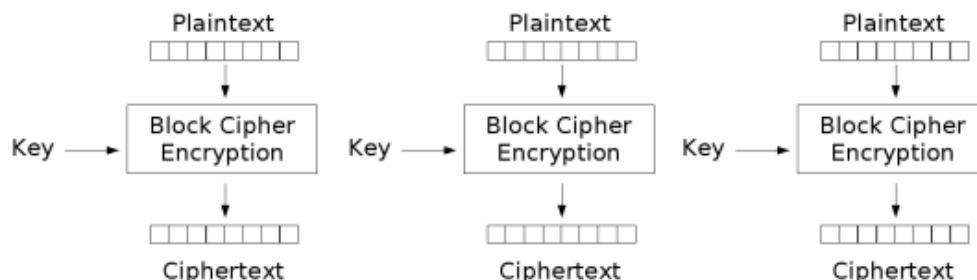
Cel ochrony danych

- poprawność,
- **poufność**,
- autentyczność, autorstwo,
- ...

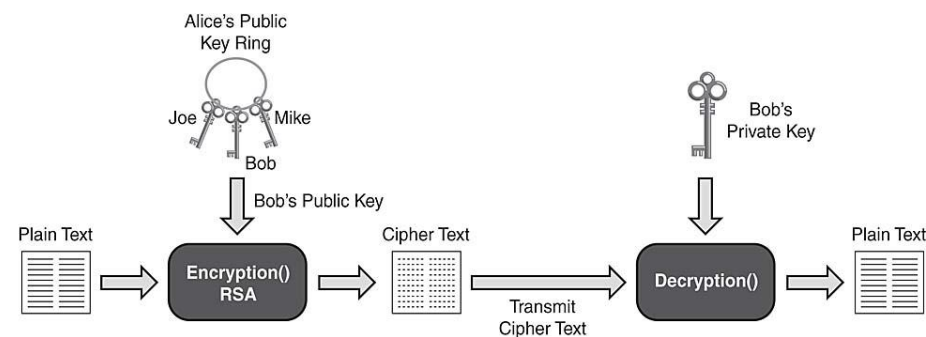
Poufność – żadna informacja na temat tekstu jawnego nie jest ujawniana

Algorytmy kryptograficzne w SZBD

- szyfrujące:
 - symetryczne:
 - blokowe
 - strumieniowe
 - asymetryczne
- podpisy cyfrowe
- funkcje skrótu:
 - MAC
 - HMAC

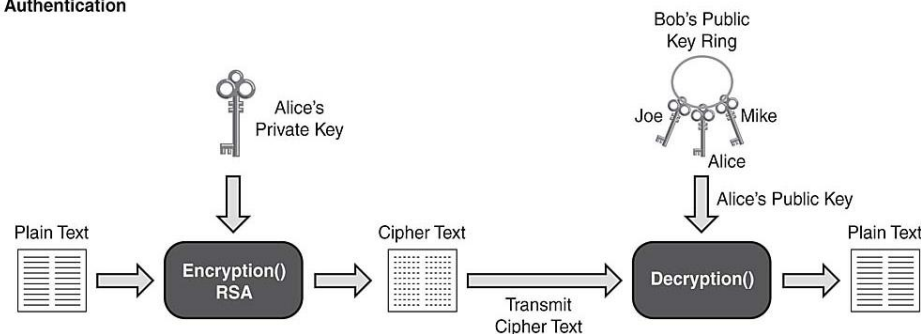


Electronic Codebook (ECB) mode encryption



Encryption

Authentication



Symetryczne vs. asymetryczne

- liczba kluczy,
- rozmiary kluczy,
- poziom bezpieczeństwa,
- szybkość działania,
- zastosowanie.

Algorytmy w bazach danych

SZBD	Symetryczne	Asymetryczne	Funkcje skrótu
Ms SQL Server	DES, 3DES AES, RC2 RC4	RSA	MD5
Oracle	3DES, AES		MD4, MD5, SHA-1
MySQL	3DES, AES		SHA-1, SHA-2, SHA-160
DB2	RC2		
PostgreSQL	AES, 3DES, CAST5, Blowfish	PGP Public- Key	MD5, SHA-1 SHA-2, SHA-3

Przykład - MsSQL

	Column Name	Data Type	Allow Nulls
id		int	☐
pesel		varbinary(256)	☐
imie		varchar(30)	☐
nazwisko		varchar(50)	☐
data_urodzenia		date	☒
plec		char(1)	☒
pensja		varbinary(256)	☒
pensja_plain		money	☒

	Column Name	Data Type	Allow Nulls
id		int	☐
pesel		char(11)	☐
imie		varchar(30)	☐
nazwisko		varchar(50)	☐
data_urodzenia		date	☒
plec		char(1)	☒
pensja		money	☒

SELECT [id],[pesel],[imie],[nazwisko],[data_urodzenia],[plec],[pensja]
FROM [encrypted].[dbo].[Pracownicy]

Results		Messages					
	id	pesel	imie	nazwisko	data_urodzenia	plec	pensja
1	26	0x01000000EE80376AE9FDC990CC59E1B269C6E6184735494B...	Jan	Kowalski	1979-06-11	M	0x003002A7091C814CB3EF7434892DC2750100000017501C7934411C8D5...
2	27	0x01000000CCECD9B57B9FFC8E31F334DC938D7DA7AC6FD93...	Anna	Kwiatkowska	1979-06-11	K	0x003002A7091C814CB3EF7434892DC275010000007869EF9E335939572...
3	28	0x01000000DAA4F3DF61003D28AB3AA4113C5435A9072F8F34...	Marcin	Nowak	1995-04-30	M	0x003002A7091C814CB3EF7434892DC275010000004CD7746F0A1DEDAA...
4	29	0x01000000717D7A4AA38F437005D72A49E4994DE24CE39457...	Malgorzata	Blazej	2002-02-28	K	0x003002A7091C814CB3EF7434892DC27501000000827249330678A052F...
5	30	0x0100000010E5C5D0FFC2C8F4A4650B2F73910268C7B3E715...	Krzysztof	Jarzyna	1994-11-26	M	0x003002A7091C814CB3EF7434892DC275010000006357E3157FF254411...
6	31	0x010000006BD05367D9AAF08733C256E259E8BE6B1311F121...	Wanda	Nowak	1965-07-01	K	0x003002A7091C814CB3EF7434892DC2750100000038736CB0F38E26519...

Konsekwencje szyfrowania

- struktura szyfrogramu,
- nadmiarowość,
 - rozmiar szyfrogramu,
 - dodatkowe informacje,
- „dziwne” typy danych,
- wyszukiwanie,
- wnioskowanie,
- dane są bezpieczne?

Przykład – DB2

```
SELECT a.name, decrypt_char(a.ssn) FROM emp a, empProject b  
WHERE a.ssn = b.ssn and b.project = 'UDDI Project';
```

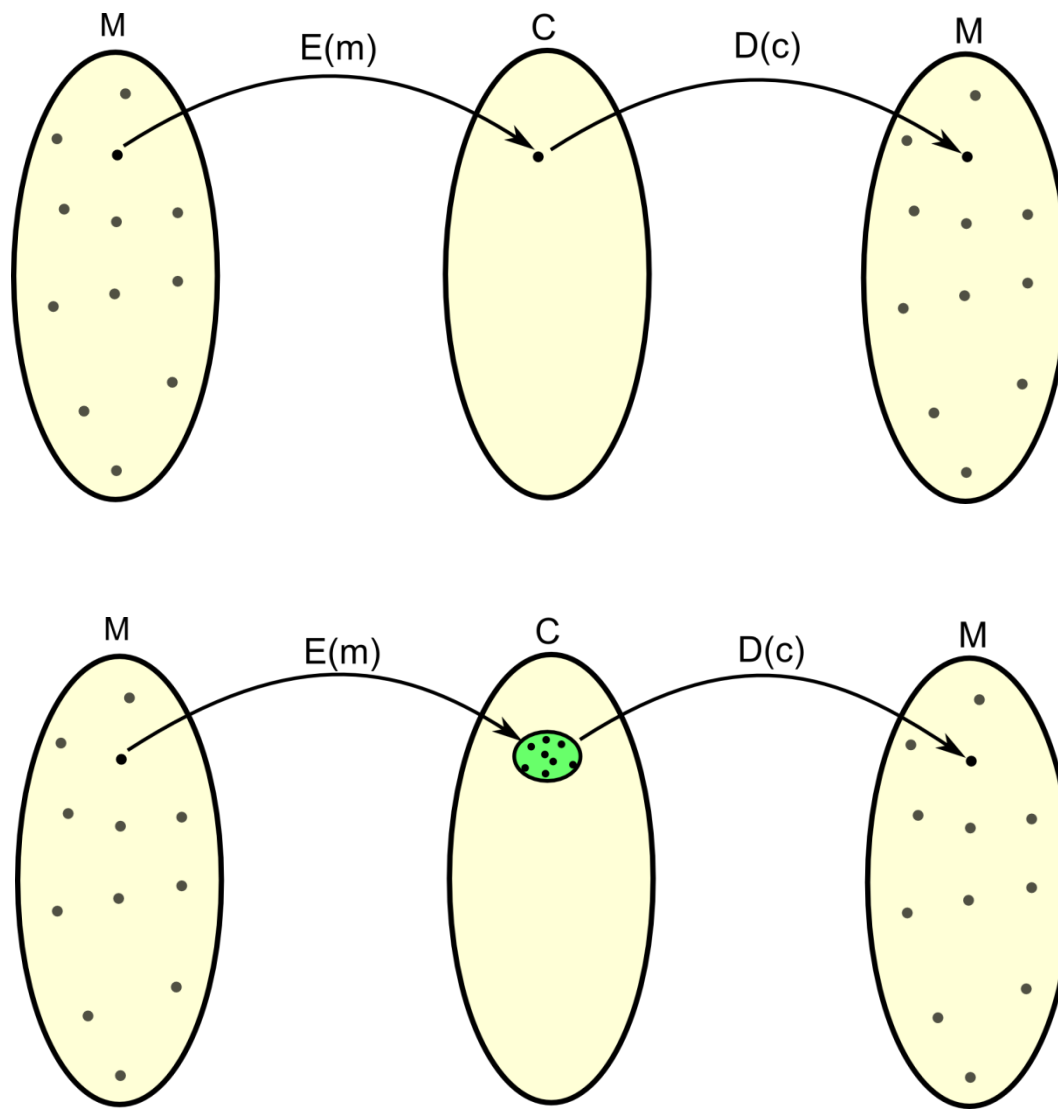
```
SELECT projectName FROM empProject  
WHERE ssn = encrypt('480-93-7558');
```

The following is an example of how **not** to write the two queries

```
SELECT a.name, decrypt_char(a.ssn) FROM emp a, empProject b WHERE  
decrypt_char(a.ssn) = decrypt_char(b.ssn)  
and b.project = 'UDDI Project',
```

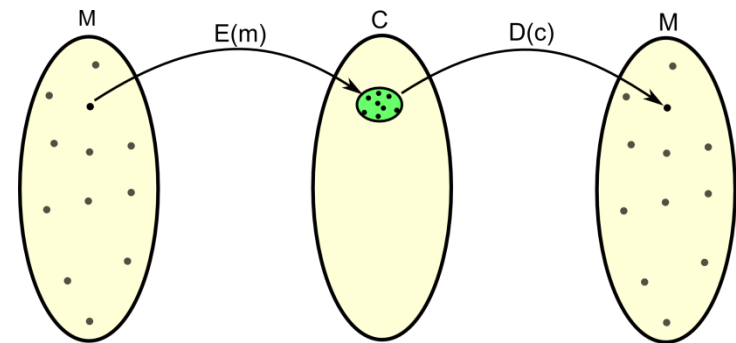
```
SELECT projectName FROM empProject  
WHERE decrypt_char(ssn)= '480-93-7558'
```

Rodzaje szyfrowania



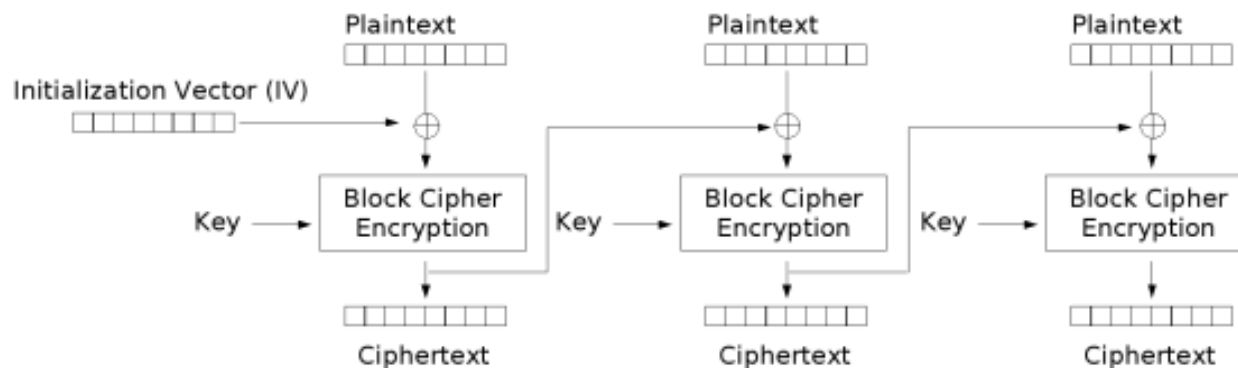
Deterministyczne czy nie?

- porównywanie,
- wyszukiwanie,
- Indeksowanie,
- złączenia,
- „podobieństwo” danych,
- poufność,



Deterministyczne, można przerobić

- losowość



Cipher Block Chaining (CBC) mode encryption

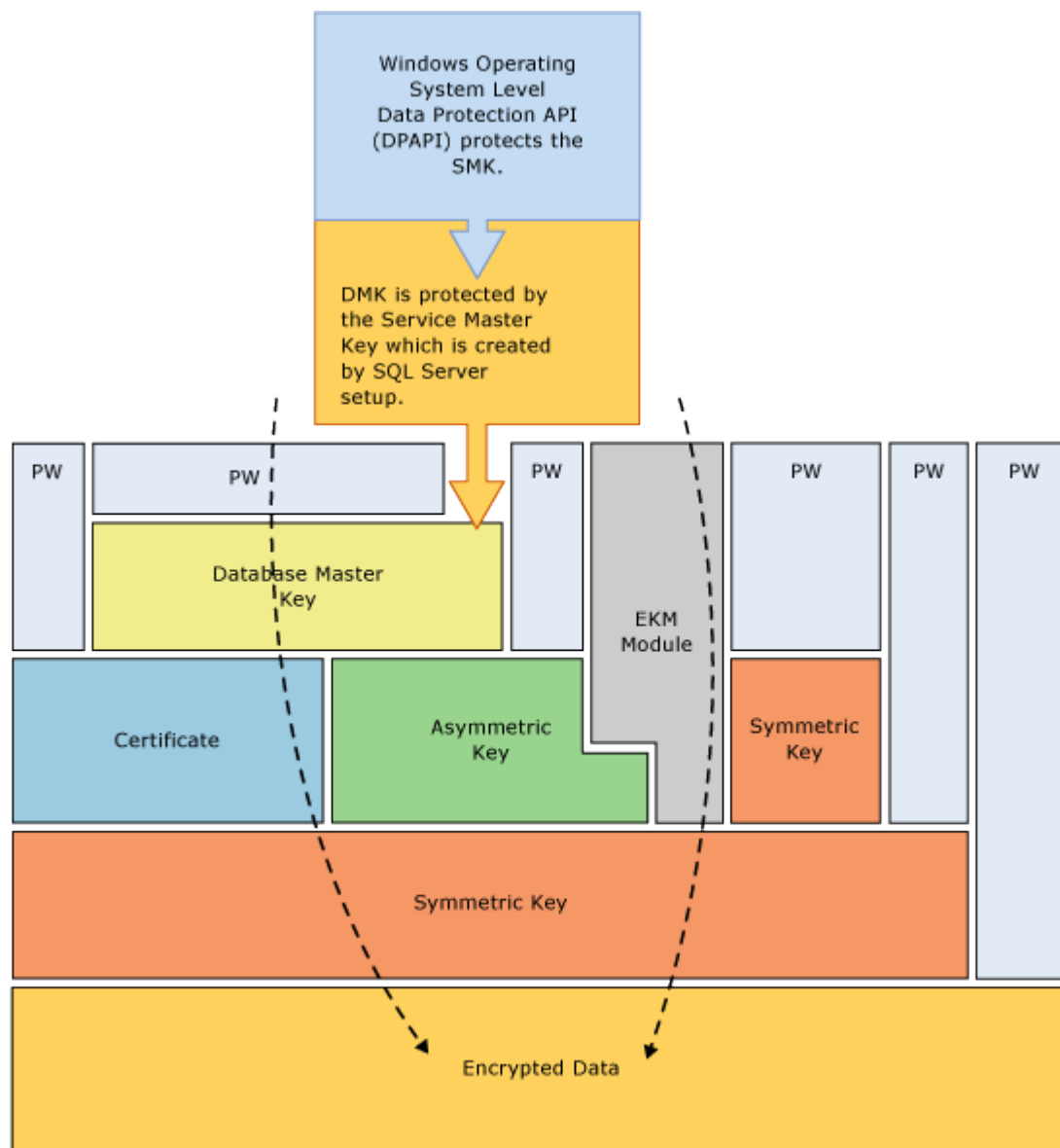
Algorytmy wymagają kluczy

- hasła
- klucze

Jak bezpiecznie przechowywać hasła i klucze?

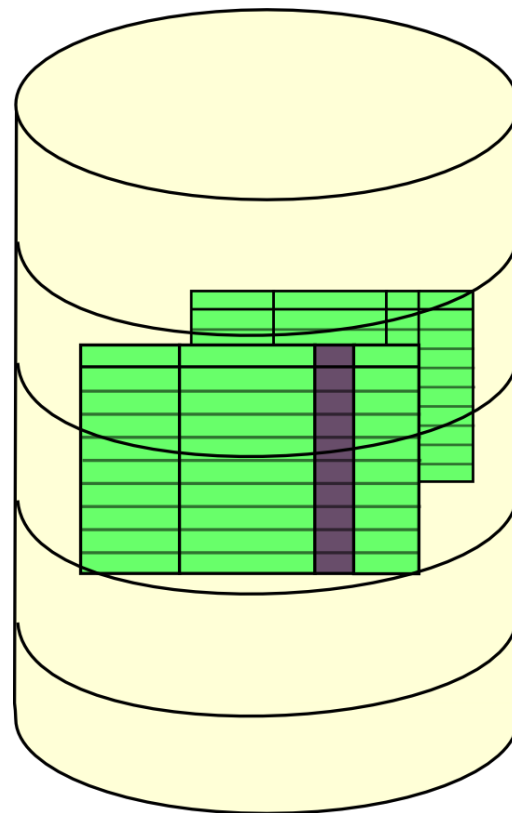
Gdzie je przechowywać?

Hierarchia kluczy



Tryby szyfrowania

- cell-level
- TDE
- file system



Cell-level vs. TDE

- wydajność,
- zakres szyfrowania,
- konsekwencje stosowania,
- dostęp do danych,
- ataki,

Cell - level	TDE
20% wolniejsze	kilka procent wolniejsze,
zmiana struktury bazy danych	28% w najgorszym przypadku
zmiana typów – pamiętanie oryginalnych, rzutowanie	niezmienna struktura i typy
indeksy mogą nie działać	pełna funkcjonalność obiektów SZBD
klucze obce nie działają	może wykorzystywać szyfrowanie sprzętowe

Wyszukiwanie

- jak szukać w danych zaszyfrowanych?

```
SELECT * FROM Table
```

```
WHERE pesel=ENCRYPT('87100565784')
```

```
SELECT * FROM Table
```

```
WHERE DECRYPT(pesel)='87100565784'
```

- usprawnienia:
 - funkcje skrótu
 - filtry Blooma
 - szyfry homomorficzne

Inne algorytmy

- MsSQL
 - SIGNBYCERT, SIGNBYASYMKEY
 - VERIFYSIGNEDBYCERT, VERIFYSIGNEDBYASYMKEY
 - CRYPT_GEN_RANDOM
 - obfuskacja
- MySQL
 - ENCODE, DECODE

Bezpieczeństwo algorytmów

- DES
- RC4 (MsSQL)
- RSA
- MD4, MD5, SHA-1

Podsumowanie

- narzut obliczeniowy i pamięciowy,
 - Oracle (column TDE) – od 1 do 52 dodatkowych bitów na tekst jawny, $\approx 5\%$ wydajności
 - MsSQL (cell-level) – kilkadziesiąt bajtów na tekst jawny, do 20% wydajności
- ograniczenia wyszukiwania, indeksowania, łączenia,
- zmiana struktury bazy danych i zapytań,
- szyfrowanie istniejących tabel z danymi,
- algorytm i tryb szyfrowania,
- ochrona transmisji do SZBD,
- dokumentacje SZBD,

Co i kiedy szyfrować

- im mniej tym lepiej,
- duże domeny,
- wymogi prawne, zalecenia:
 - obrazy DICOM,
 - numery kart kredytowych, SSN, PESEL,
- wyszukiwanie danych – exact i range,
- złączenia,
- algorytmy symetryczne preferowane

Linki

- MySQL:
 - https://dev.mysql.com/doc/refman/5.5/en/encryption-functions.html#function_encode
- Oracle:
 - http://docs.oracle.com/cd/B19306_01/network.102/b14268/asotrans.htm#BABDACEG
 - <http://my.safaribooksonline.com/book/databases/oracle-pl-sql/0596005873/data-encryption-and-hashing/oracleplsqldb-chp-4-sect-3>
 - <http://www.oracle-base.com/articles/10g/transparent-data-encryption-10gr2.php>
 - <http://www.oracle.com/technetwork/database/security/tde-faq-093689.html>
 - <http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf>
- DB2:
 - <http://www.ibm.com/developerworks/data/library/techarticle/benfield/0108benfield.html>
- MsSQL:
 - [http://technet.microsoft.com/en-us/library/ms189586\(v=sql.110\).aspx](http://technet.microsoft.com/en-us/library/ms189586(v=sql.110).aspx)
 - <http://technet.microsoft.com/en-us/library/ms188357.aspx>
 - <http://msdn.microsoft.com/pl-pl/library/ms173744.aspx>
 - <http://msdn.microsoft.com/pl-pl/library/ms187920.aspx>
 - [http://technet.microsoft.com/pl-pl/library/hh264548\(v=vs.100\).aspx](http://technet.microsoft.com/pl-pl/library/hh264548(v=vs.100).aspx)
- IP v6:
 - <http://blogs.cisco.com/news/ipv6-deployment-threshold-reached/>
 - <http://www.google.com/ipv6/statistics.html#tab=per-country-ipv6-adoption>