PODSTAWY KRYPTOGRAFII

PIOTR DOBOSZ

CZYM JEST KRYPTOGRAFIA?

- Metoda konwersji zrozumiałego tekstu na nieintuicyjną formę
- Szereg nakładających się procesów mający na celu ochronić integralność przechowywanej informacji
- Cryptography – 'crypt-' oznacza ukryte, schowane; zaś '-graphy' oznacza pisanie, zapis

JAK ZDEFINIOWAĆ KRYPTOGRAFIĘ?

- Techniki pochodzące od matematycznych obliczeń koncepyjnych i warunkowych – algorytmy
- Koncepcja zakłada, że zaszyfrowane dane będą, bez znajomości warunków i koncepcji, bardzo trudne do odszyfrowania
- Algorytmy używane w kryptografii są deterministyczne (znaczenie słowa)
- Znajduje zastosowanie w podpisach cyfrowych, weryfikacji poprawności danych, szyfrowania danych poufnych, generowanie kluczy dostępowych, potwierdzeniach transakcji płatniczych

TECHNIKI KRYPTOGRAFICZNE

- Używanie tzw. Mikrokropek
- Łączenie obrazów z tekstem
- Tzw. zasalanie tekstu pierwotnego
- W podstawowej wersji wykorzystuje się tzw. mieszanie tekstu poprzez przydzielanie wartości pojedynczym znakom (bądź grupom znaków), przydzielanie grupy znaków do wskazanego znaku itp.
- Proces może być odwracalny lub nie!

HISTORIA KRYPTOGRAFII

- Już w starożytności wykorzystywano metody kryptograficzne celem ochrony określonych informacji...
- … lub jak urzędnik Khnumhotep II (Nomarch) w 3900 roku P.N.E. - do upiększania tekstu (zastępowanie powtarzających się wyrazów)
- W Mezopotamii (3500 P.N.E.) użyto technik kryptograficznych celem ochrony formuły szkliwa garncarskiego
- W Sparcie stosowano zapis wiadomości na pergaminie dostosowanym wielkościowo do pewnej fromy (najczęściej cylindra); tylko przyłożenie tak zapisanego pergaminu do drugiego, identycznego walca, umożliwiał odczyt wiadomości
- Szyfrowano wiadomości wojskowe i szpiegowskie (szyfr Cezara)

HISTORIA KRYPTOGRAFII

- Powstanie metody polialfabetycznej (Leone Alberti)
- Powstanie kodowania binarnego (Sir Francis Bacon – 1623)
- Koło szyfrujące składające się z 36 literowych pierścieni osadzonych na ruchomych kółkach (Thomas Jefferson – 18 wiek)

ZAPIS BINARNY

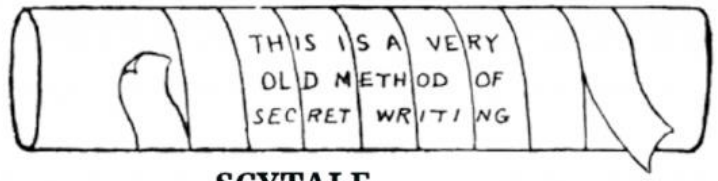
Klucz

Litera:	a	b	c	d	e	f	g	h
Kod:	AAAAA	AAAAB	AAABA	AAABB	AABAA	AABAB	AABBA	AABBB
Litera:	i-j	k	l	m	n	o	p	q
Kod:	ABAAA	ABAAB	ABABA	ABABB	ABBAA	ABBAB	ABBBA	ABBBB
Litera:	r	s	t	u-v	w	x	y	z
Kod:	BAAAA	BAAAB	BAABA	BAABB	BABAA	BABAB	BABBA	BABBB

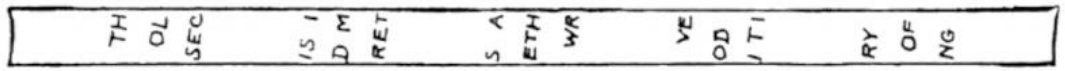
PRZYKŁADY SZYFROWANIA DANYCH

ATBASH CIPHER

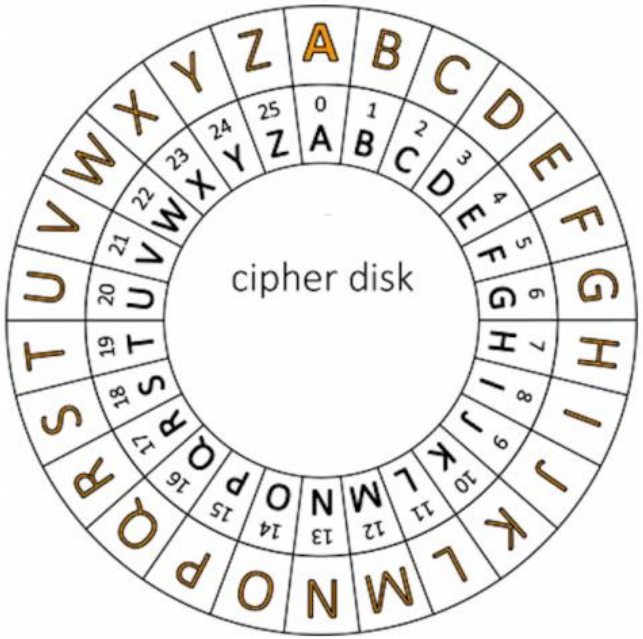
Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A



SCYTALE



CAESAR CIPHER



POLYBIUS SQUARE

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

SZYFROWANIE DANYCH – DYSK JEFFERSONA

VIGENERE CIPHER

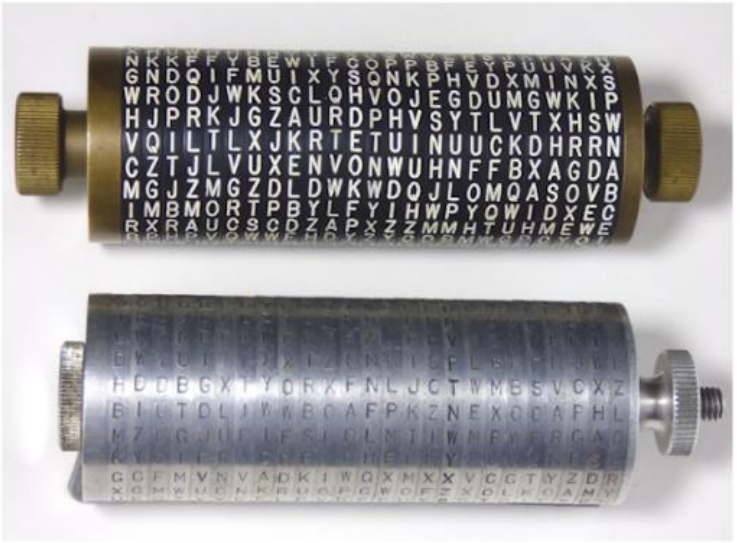
Message Character

Key Character	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Using the Table

Encryption		Decryption	
Message:	S E N D H E L P	Ciphertext:	T Y Y J L F F A
Key:	B U L G E B U L	Key:	B U L G E B U L
Ciphertext:	T Y Y J L F F A	Message:	S E N D H E L P

JEFFERSON DISK CIPHER



PLAYFAIR CIPHER

Plain Text: "instrumentsz"

Encrypted Text: gatlmzclrqtx

in:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

st:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

ru:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

me:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

nt:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

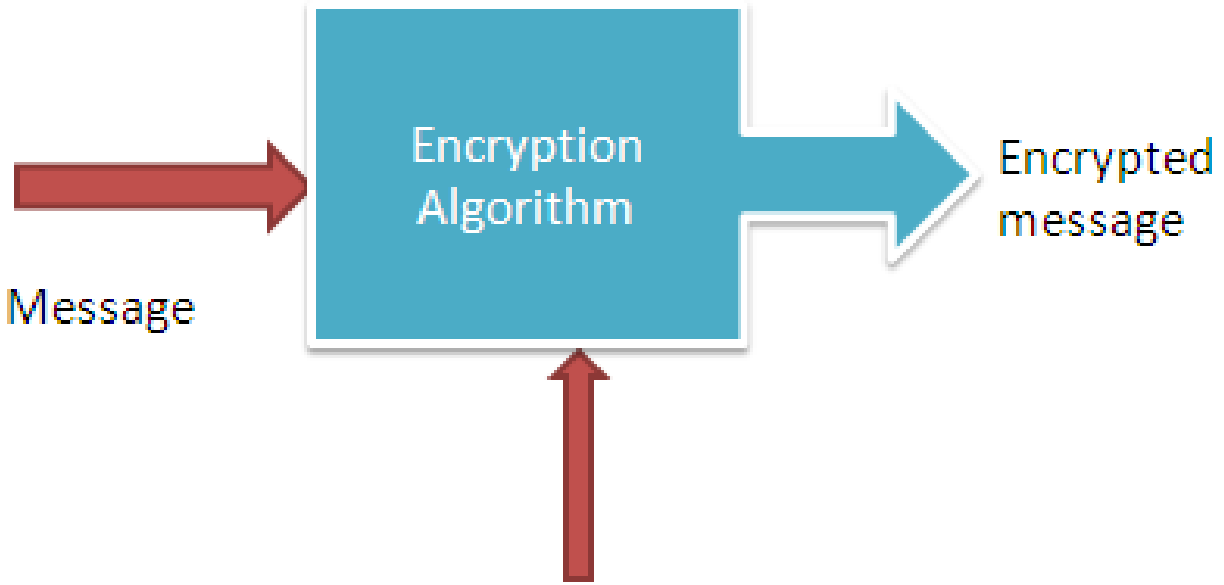
sz:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

HISTORIA KRYPTOGRAFII – INFORMATYKA I WSPÓŁCZESNOŚĆ

- Wykorzystanie urządzeń elektroniki celem szybkiego szyfrowania danych
- Możliwość dodawania dowolnych, ograniczonych jedynie mocą obliczeniową, tzw. Kluczy szyfrujących
- Możliwość łączenia ze sobą dodatkowych technik szyfrujących, jak tablice przestawne, łączenie tekstu z obrazami, przelatania danych innymi danymi itp.

PRZYKŁAD UŻYCIA KLUCZA SZYFRUJĄCEGO



128 bit key

For example: 00001111000011110000
00001111000011110000000011110000111
10000000011110000111100000000111100
00111100000000111100001111000011111
111

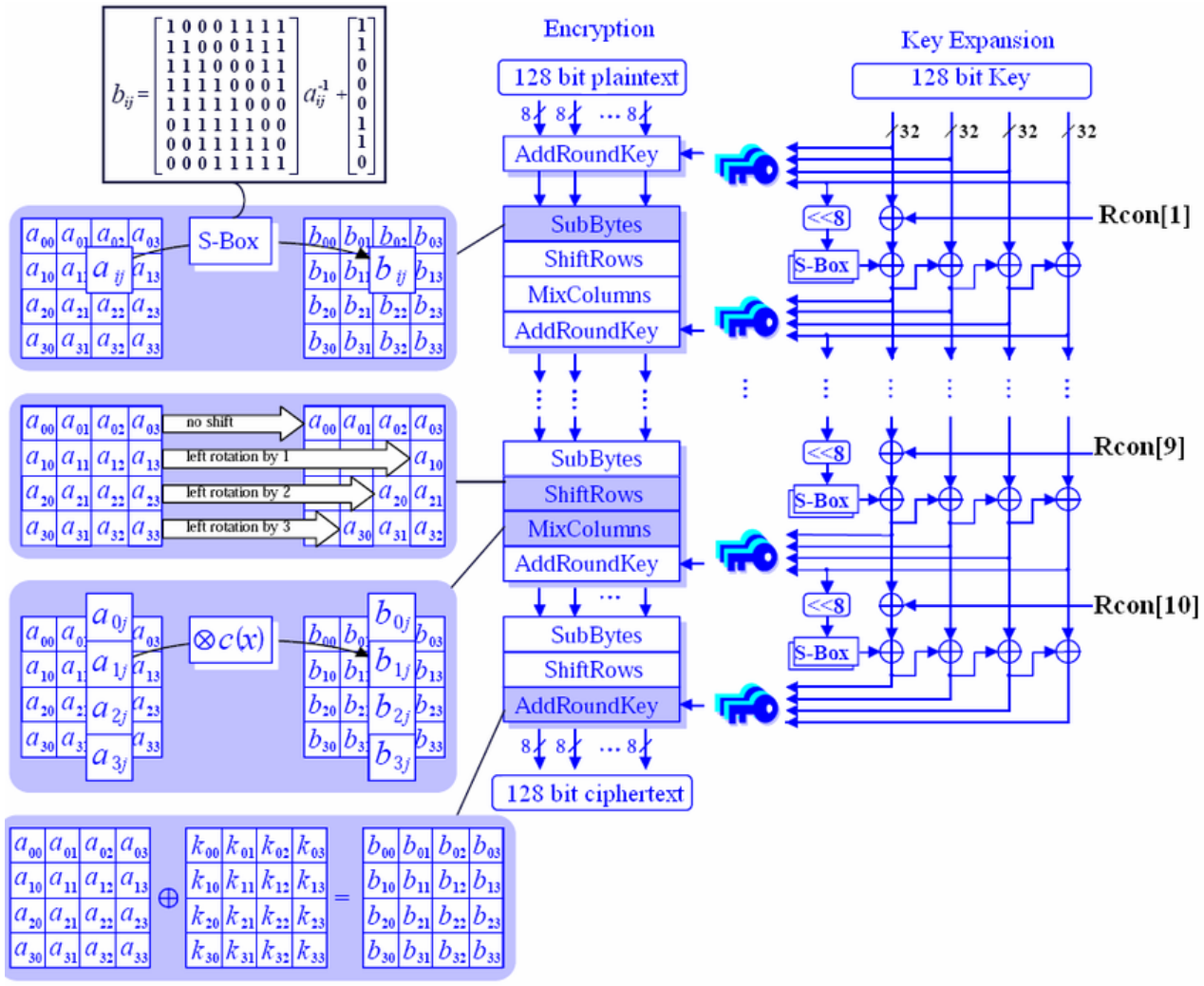
PRZYKŁADY SKOPLIKOWANIA KLUCZY SZYFRUJĄCYCH

- https://i.stack.imgur.com/9jeNJ.jpg

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

PRZYKŁAD DZIAŁANIA KLUCZA 128 BITOWEGO

- https://www.researchgate.net/profile/Mehdi_Baboli/publication/261364082/figure/fig1/AS:392378570559496@1470561749684/Functional-block-diagram-of-AES-128.png



ŁAMANIE SZYFRU 128 BITOWEGO

- https://lh5.ggpht.com/_Wom5eMghH20/S8TpWVHX2uI/AAAAAAAAA1Y/moTJ3XUPff8/image_thumb%5B4%5D.png?imgmax=800

Computation Reference for 128-Bit Key Crack Example	
People	7.00E+09
Computers per person	10.00
Computers	1.00E+09
Combos per second per computer	7.00E+19
Total combos per second	7.00E+19
Seconds per year	3.15E+07
Total combos per year	2.22E+12
128-bit key combos (*50%)	1.70E+38
Years to crack	7.66E+25

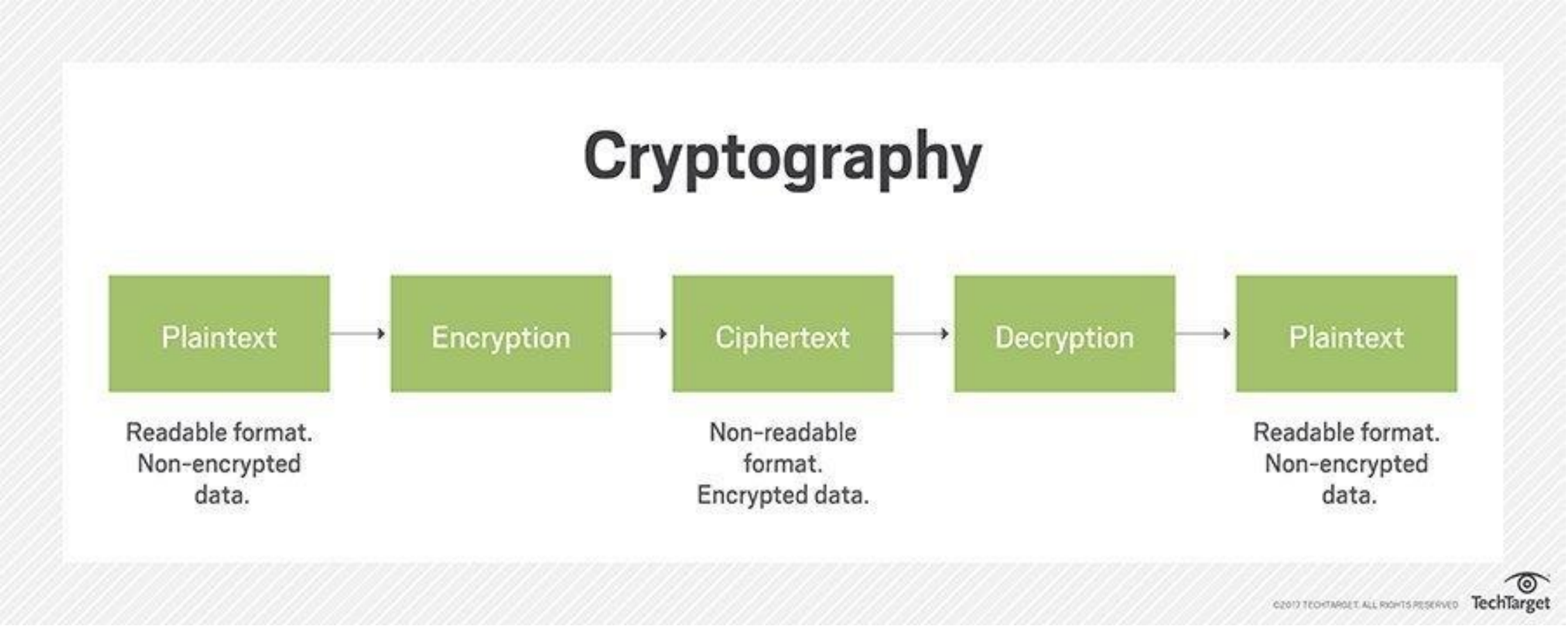
CELE KRYPTOGRAFII

- Poufność (Confidentiality)
- Integralność (Integrity)
- Niezaprzeczalność (Non-repudiation)
- Poświadczenie/autentykacja (Authentication)

SYSTEM KRYPTOGRAFICZNY

- Rozwiązania kryptograficzne spełniają przeważnie tylko część wcześniej wskazanych celów i zasad
- Często jednak uwzględniają słabość systemu – czynnik ludzki
- Standardowo uwzględnia się regulacje co do zachowań użytkownika systemu, jak poufność przechowywania hasła, zasady pracy z systemami poufnymi, zachowanie w tajemnicy stosowanych procedur w systemach zabezpieczeń przedsiębiorstwa

DZIAŁANIE SYSTEMU KRYPTOGRAFICZNEGO



ALGORYTM KRYPTOGRAFICZNY

- Kryptosystem składa się z szeregu procedur zwanych algorytmami kryptograficznymi/szyfrującymi
- Algorytmy mają zapewniać bezpieczne składowanie i/lub przekazywanie informacji; w przypadku informatyki tyczy się to urządzeń elektronicznych
- Podział algorytmów na algorytmy szyfrujące, potwierdzające oraz służące wymianom kluczy
- Przykładowe rozwiązanie kryptograficzne: Advanced Encryption Standard (AES), Data Encryption Standard (DES), DES3, Rivest-Shamir-Adleman (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA), Digital Signature Algorithm (DSA)
- Funkcje mieszające: SHA-1 (Secure Hash Algorithm 1), SHA-2 i SHA-3; to także MD5 (niezalecany)

SŁABE STRONY KRYPTOGRAFII

- Słabsze klucze mogą być łatwo łamane celem pozyskania wrażliwych danych
- Błędy i niedociągnięcia istniejących algorytmów mogą umożliwiać odszyfrowanie danych bez posiadania odpowiednich uprawnień/kluczy
- Niektóre rozwiązania pozwalają na pozyskanie kluczy uniwersalnych
- Zagrożenie ze strony komputerów kwantowych

KRYPTOANALIZA

- Nauka, której celem jest badanie systemów kryptograficznych i pozyskiwanie informacji o ich słabościach
- Może dać dostęp do danych nienależycie zabezpieczonych bądź zabezpieczonych słabej jakości szyfrem
- Często brane jest pod uwagę pozyskanie informacji poprzez tzw. atak boczny (side-channel attack)
- Często analizuje się ataki wykorzystujące luki w implementacji algorytmu (nie zaś jego matematycznej postaci)
- Kryptoanaliza liniowa, różnicowa, statystyczna
- Ataki typu brute force

SCHEMAT ATAKU

- https://d3i71xaburhd42.cloudfront.net/45e5d504a986c4f17834b00fa01fbbc409cd8276/4-Figure1-1.png

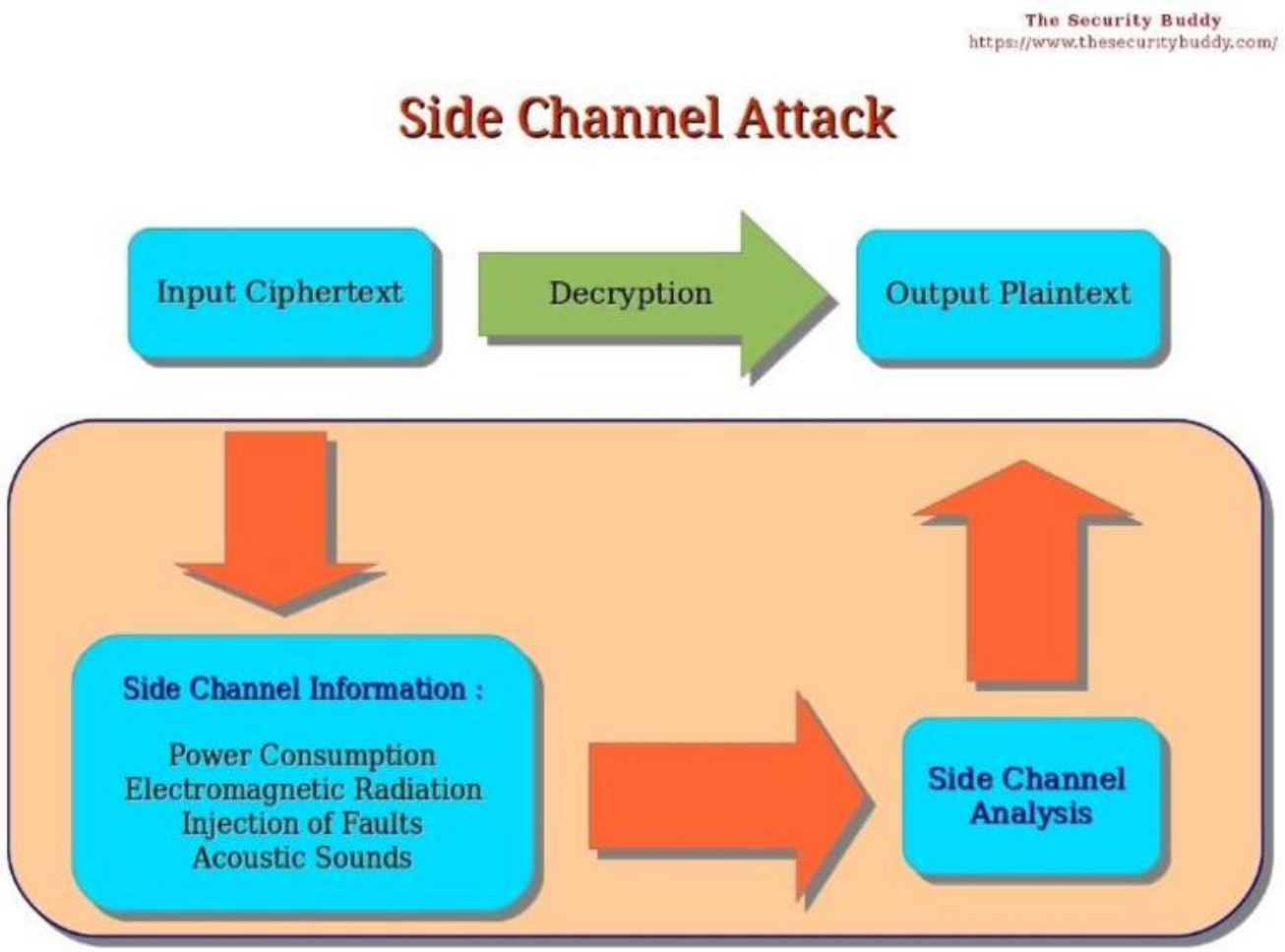
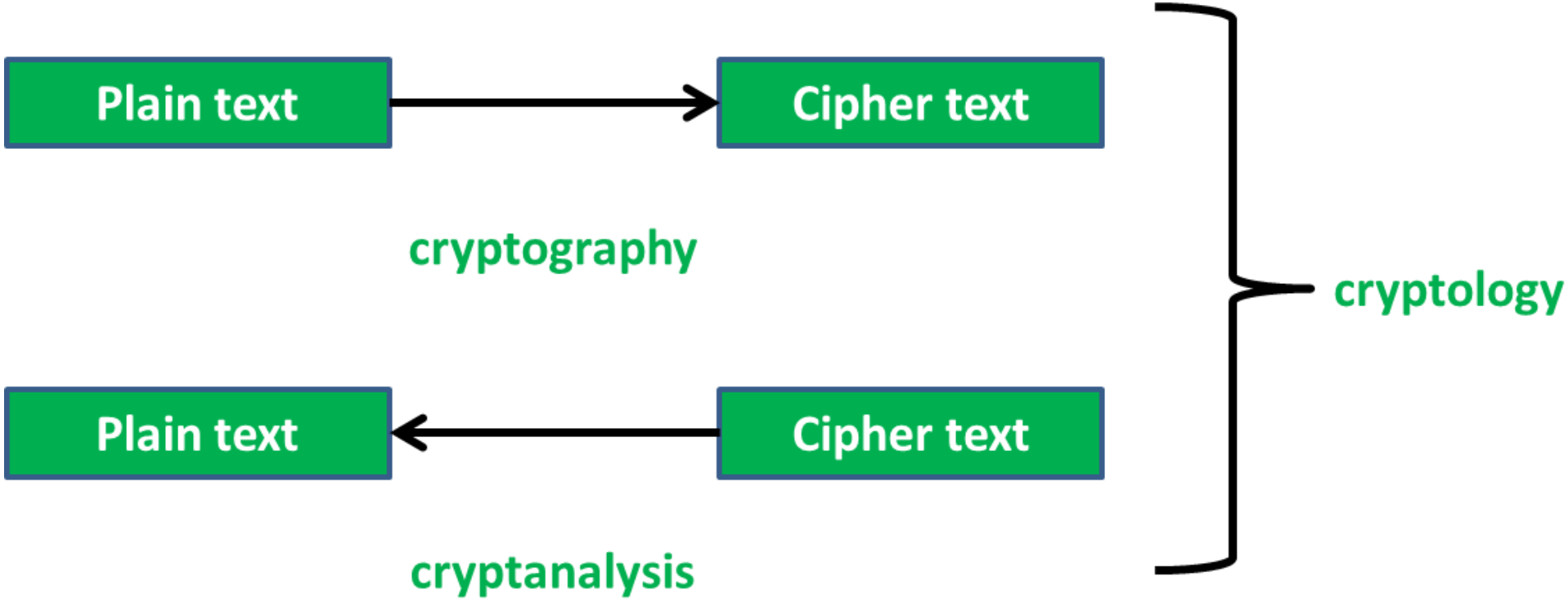


***Figure 1**. Side channel attacks[41]*

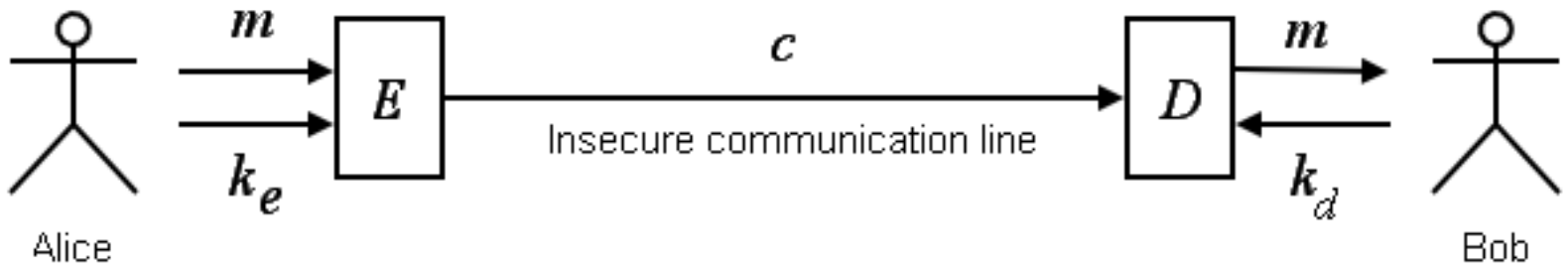
KRYPTOGRAFIA I KRYPTOANALIZA A KRYPTOLOGIA

- Kryptologia obejmuje swoim zakresem działania kryptograficzne oraz dekryptograficzne
- Niektóre źródła wskazują na powiązania z kryptoanalizą (ze względu na działania deszyfrujące, obejmowane swoim zakresem przez kryptologię)
- Kompleksowo zajmuje się zabezpieczaniem danych różnego rodzaju (obecnie głównie elektronicznie)

KRYPTOLOGIA



DZIAŁANIE KRYPTOLOGICZNE



Alice - sender
Bob - receiver
E - encoding algorithm
k_e - encoding key
D - decoding algorithm
k_d - decoding key
m - message (a.k.a. plaintext)
c - ciphertext

$E(m, k_e) = c$
$D(c, k_d) = m$

Eve - can only listen in but can not modify c
Mallory - can listen in and modify c

KODOWANIE I SZYFROWANIE

- Kodowanie to proces zamiany jednej wartości na drugą
- Nie ma intencji bycia niezrozumianym przez ogół
- Dobrym przykładem jest alfabet Morse'a
- Albo kodowanie base64

KODOWANIE I SZYFROWANIE

- Szyfr nie ma znaczenia
- W przeciwieństwie do poprzedniego przykładu - nie ma potrzeby posiadania książki kodu
- Bazuje na przesunięciach oraz umiejętnym wplataniu (wedle algorytmu) wartości, które celem deszyfrowania, należy przeprowadzić w odwrotną stronę
- Podsumowując kodowanie bazuje na semantyce książki kodującej, zaś szyfrowanie na składni i operacjach względem pojedynczego znaku (rzadziej serii znaków).

MATERIAŁY I ŹRÓDŁA

- https://calcoolator.pl/szyfr-bacona.html
- https://en.wikipedia.org/wiki/Microdot
- https://www.bogaty.men/kryptolandia-o-potrzebach-i-historii-kryptografii/
- https://academy.binance.com/pl/articles/history-of-cryptography
- https://searchsecurity.techtarget.com/definition/cryptography
- https://www.britannica.com/topic/cryptology
- https://cs.lmu.edu/~ray/notes/cryptology/
- https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes