Wstęp do praktycznej kryptografii

Jakub Maria Juszczakiewicz

Akademickie Stowarzyszenie Informatyczne

6 marca 2012

Przebieg wykładu

Plan prelekcji

- Czym jest kryptografia?
- Szyfry i klucze
- Które hasła są lepsze?
- Zastosowania

Czym jest kryptografia?

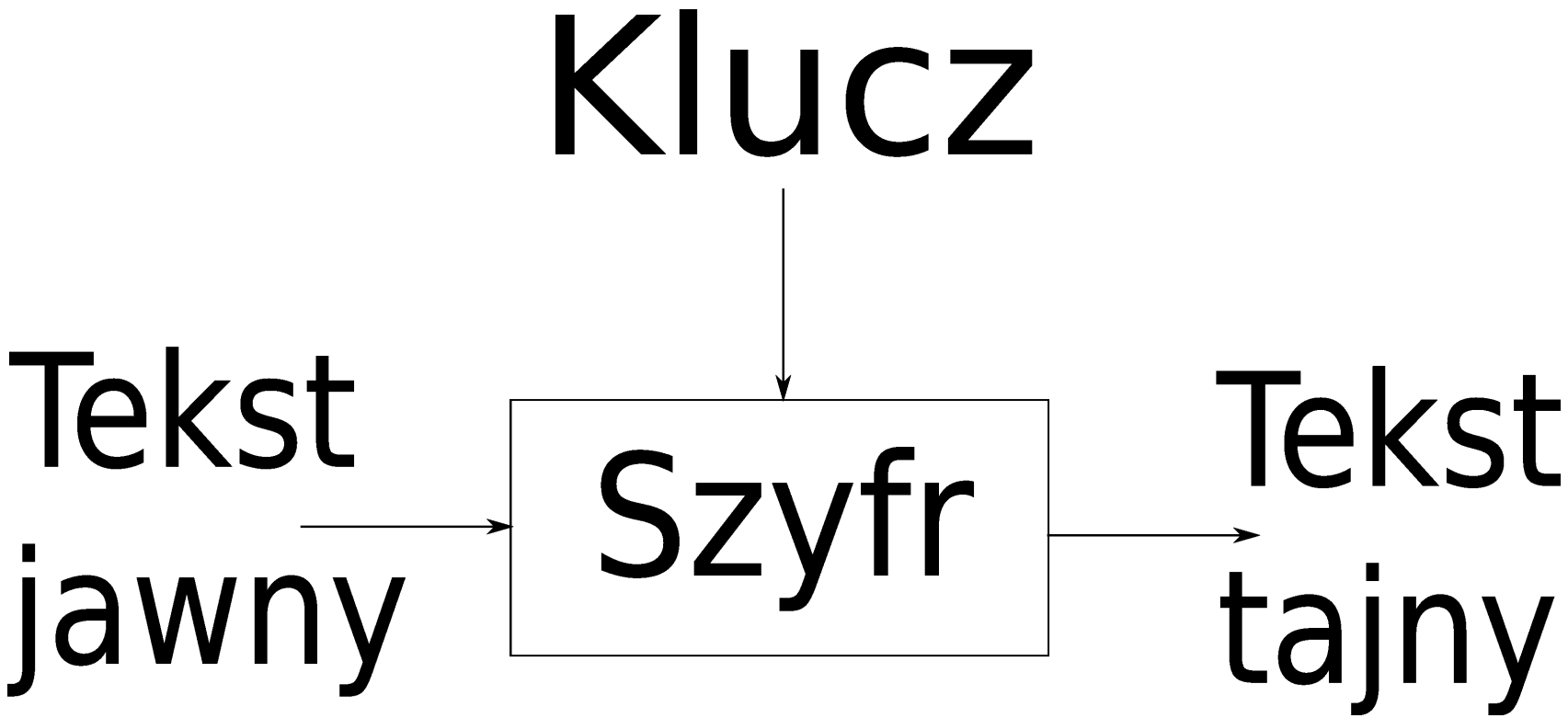
$$
\begin{aligned}
&\text{Kryptografia} \\
+\ &\text{Kryptoanaliza} \\
=\ &\text{Kryptologia}
\end{aligned}
$$

Podział szyfrów

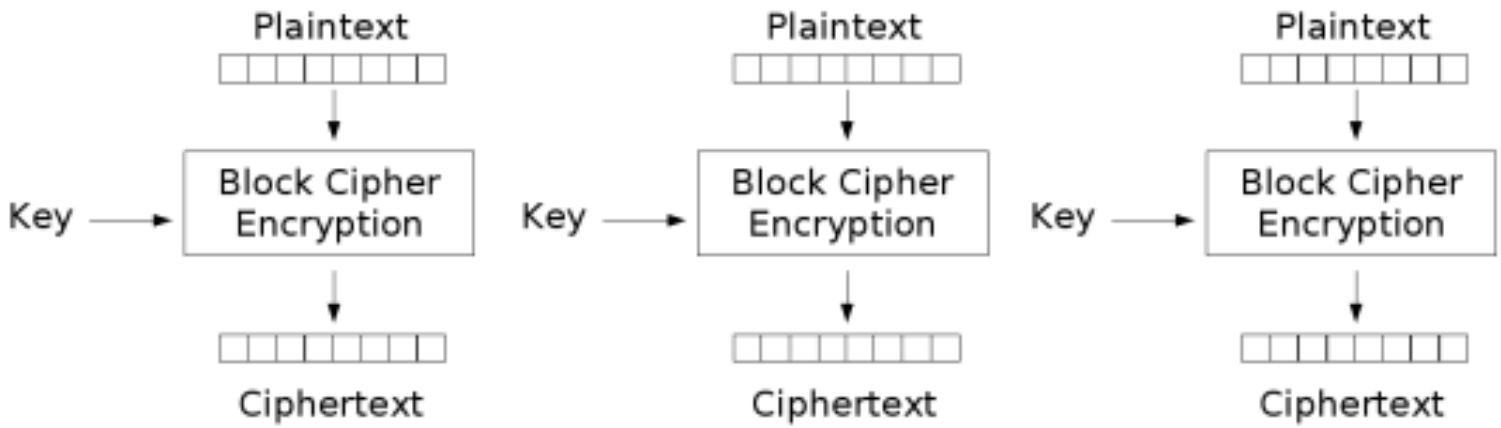
Szyfry

- Historyczne
- Symetryczne
  - Strumieniowe
  - Blokowe
- Asymetryczne

Jak działa szyfr blokowy?

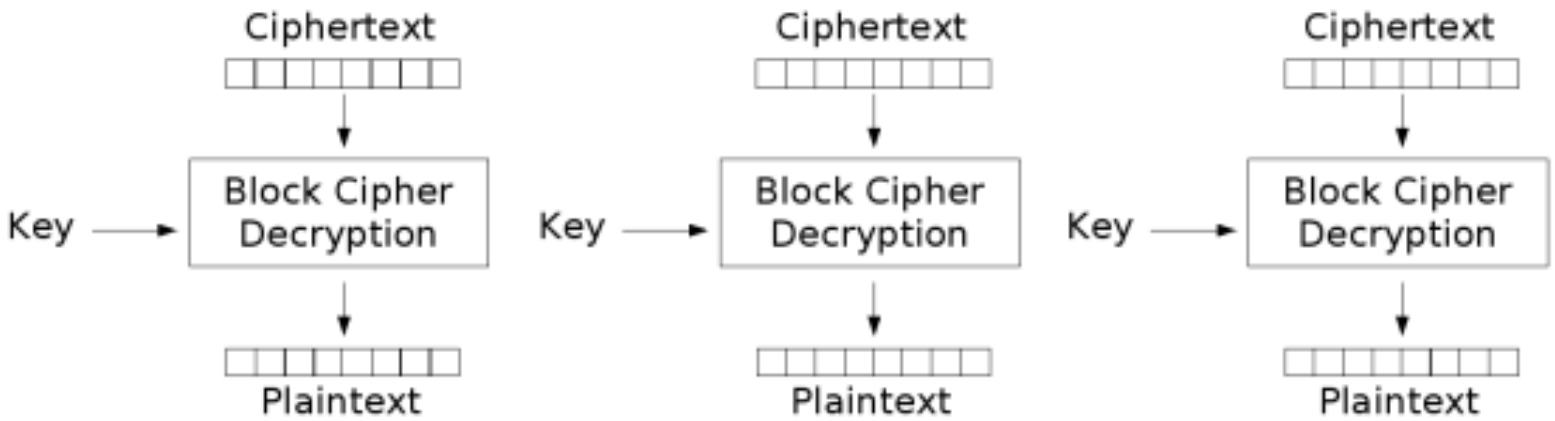


ECB - Szyfrowanie



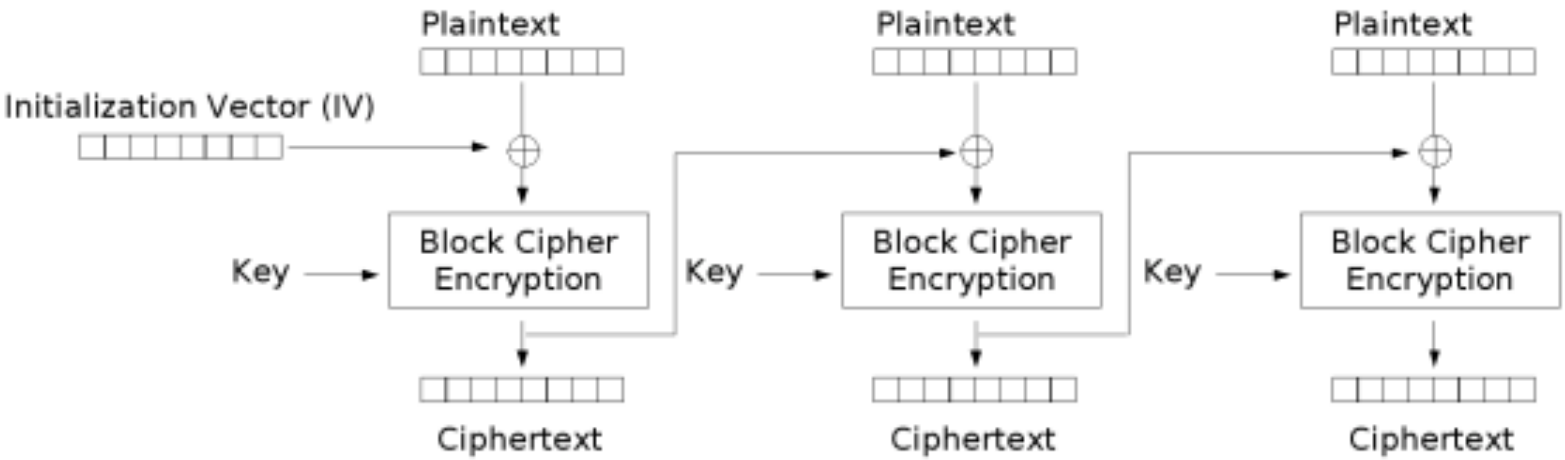
Electronic Codebook (ECB) mode encryption

ECB - Deszyfrowanie



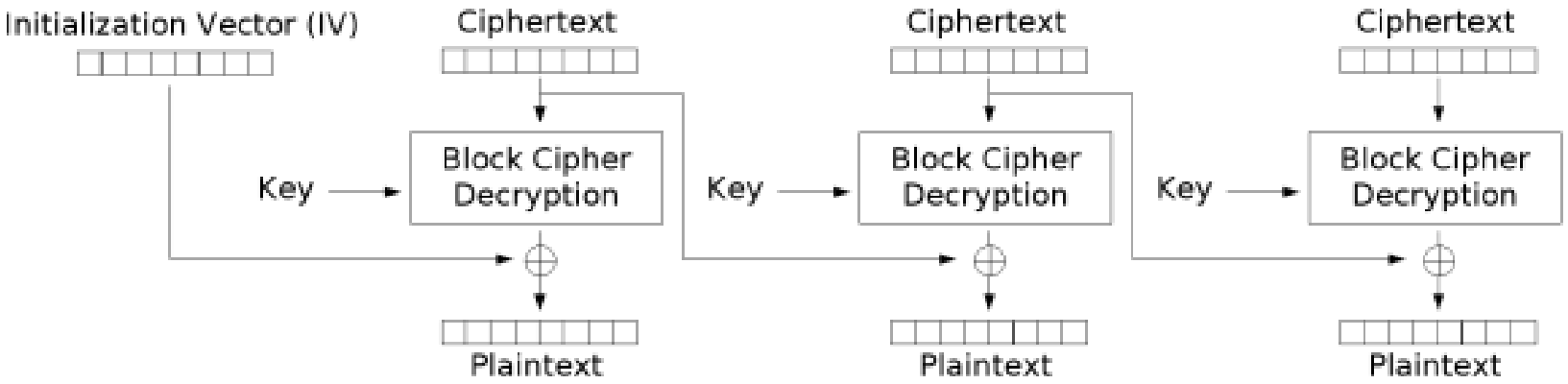
Electronic Codebook (ECB) mode decryption

CBC - Szyfrowanie



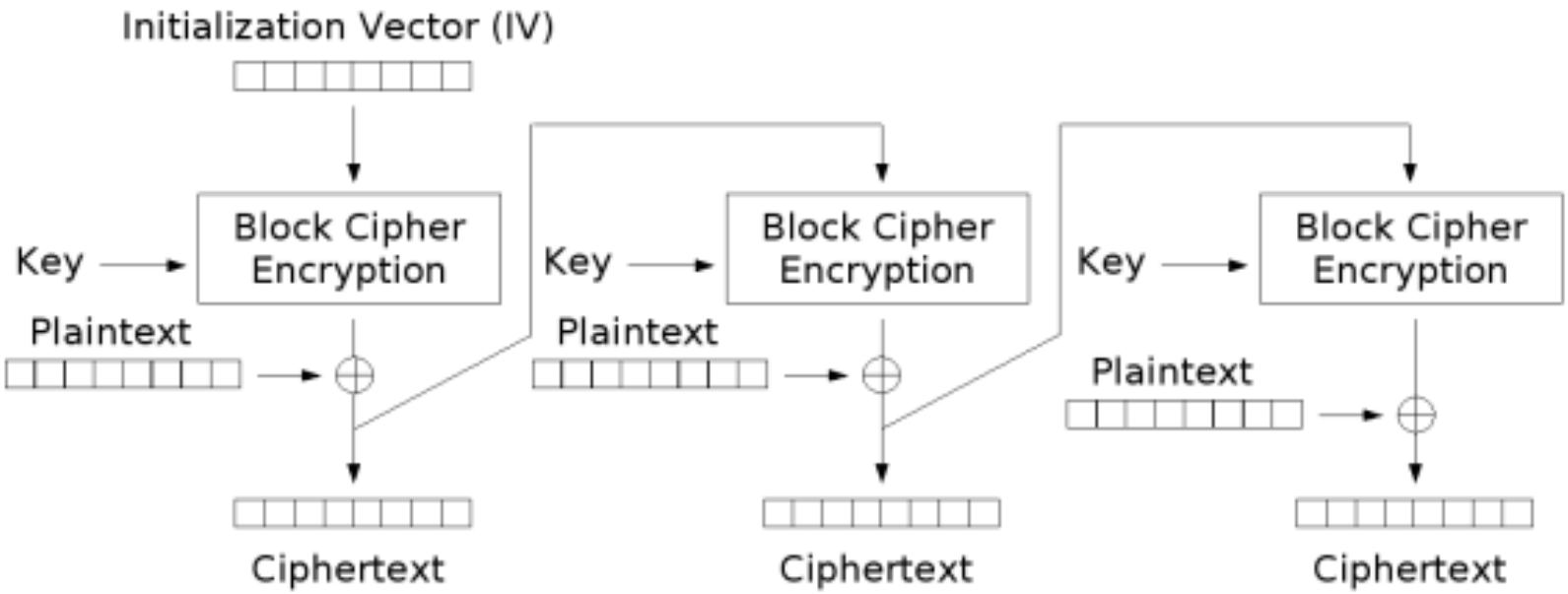
Cipher Block Chaining (CBC) mode encryption

CBC - Deszyfrowanie



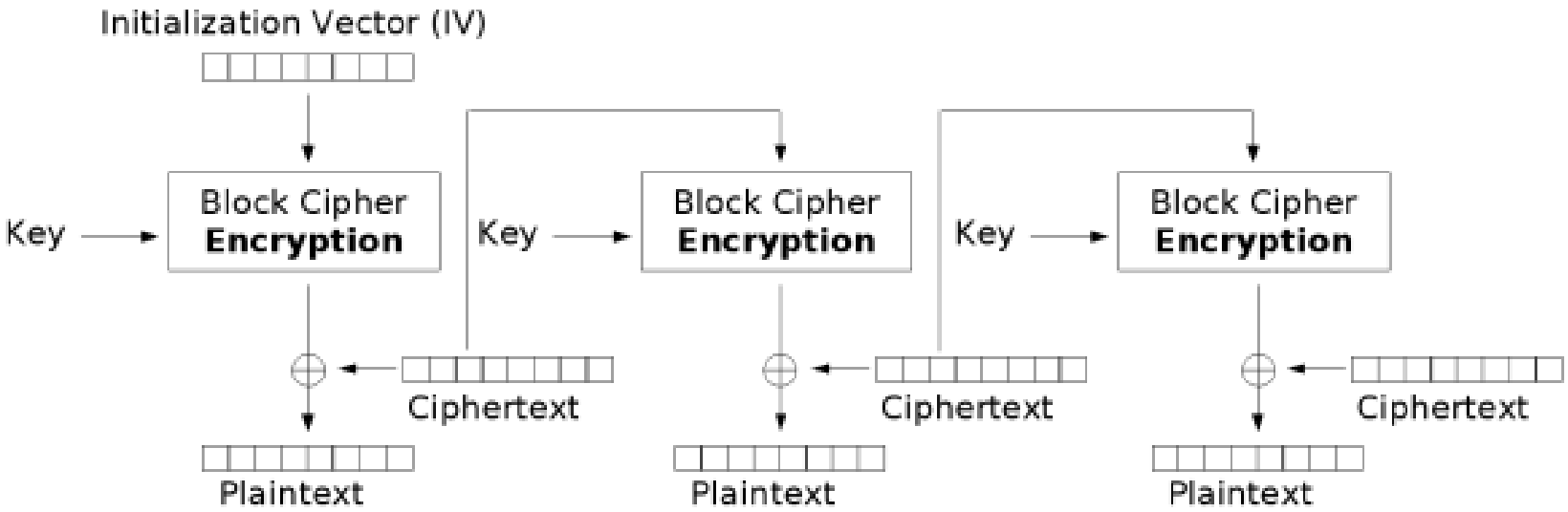
Cipher Block Chaining (CBC) mode decryption

CFB - Szyfrowanie



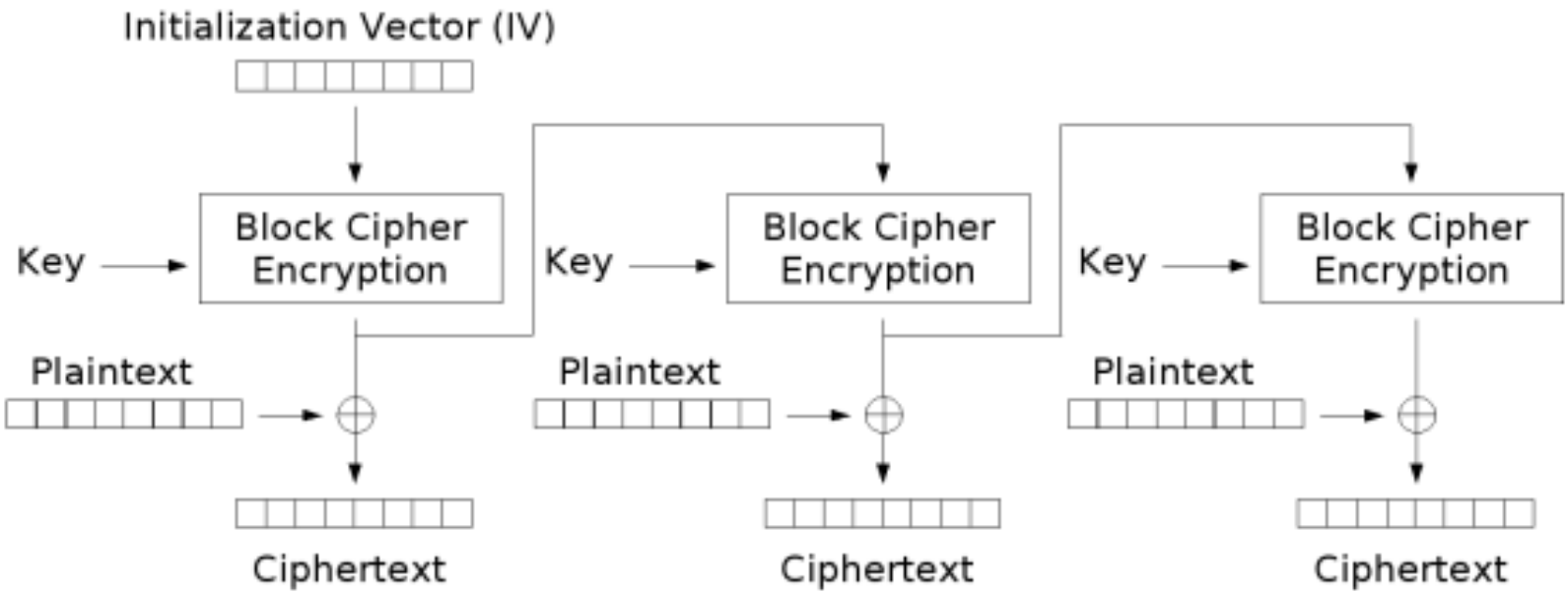
Cipher Feedback (CFB) mode encryption

CFB - Deszyfrowanie



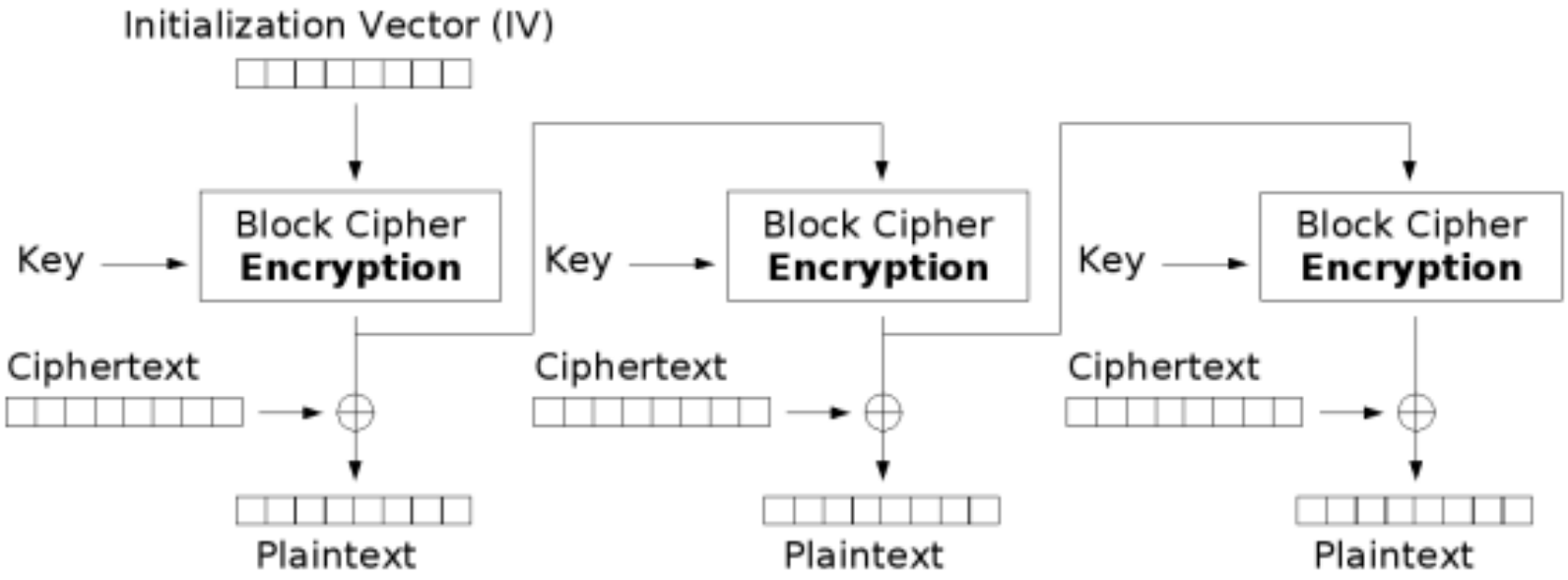
Cipher Feedback (CFB) mode decryption

OFB - Szyfrowanie



Output Feedback (OFB) mode encryption

OFB - Deszyfrowanie



Output Feedback (OFB) mode decryption

Funkcja skrótu

Przykładowe funkcje skrótu: MD4, MD5, RMD-160, SHA-1, SHA-2 (224, 256, 384, 512)

Wielkość klucza a bezpieczeństwo

Rozmiar klucza	czas sprawdzania*
32 bity	około 1 godziny 12 minuty
33 bitów	około 2 godziny 23 minuty
56 bity	2283 lata
128 bitów	10782897524556318080696079 lat

* - tępo 1 000 000 sprawdzeń na sekundę

Jakie hasła są bezpieczne?

MoCnE.#?HaSlO

tojesthasloktorelatwozapamietac

Jakie hasła są bezpieczne?

MoCnE.#?HaSlO

$100^{13} = 1000000000000000000000000000$

tojesthasloktorelatwozapamietac

$26^{31} =$

$731431714334033939007241467700152595392757 76$

Tablice tęczowe

Spreparowane tablice ze skrótami

Jak się uchronić? - Solą.

wQPMLUD3kQgz03rLxEobOg

UMI7wa7lpus4WiuwWlk1DAgkAJtzGyXi6ldWc270
ExOlz6pURJAuI1f6QZKPVPstAtU0f90wg+24jT6P
GFJyW5CjFtr63FvYrYxs7PerAQzSk2FBLKDi0CgP
Ll7WA75YLBNbeQe1NVtFwrtqfnJ3GjeJ5fwq0BgX
9ZVNR45BFR+Cvky8qtr1zrPIMIGvYLZZZORGPX4
038Mfh7qjXhaYgNqVePkhZARleFRjmPMJUr7klj
GT040zHbiUU1V87HhVfvV3pCTC1xAxXZxzgrxqDB
bZwXrEZc3AuFq0FjxQl3Yk+20hG7M6TDL5bnIGJH
OAkxLy2x0URBOnlGoHA

Szyfr którego nie da się złamać

XOR

	0	1
0	0	1
1	1	0

Szyfr strumieniowy

01000111000010100100010010101000101001 0 - wiadomość
10100110010101010101000110111101001000 0 - klucz

11100001010111111001010100010101100001 0 - szyfrogram
10100110010101010101000110111101001000 0 - klucz

01000111000010100100010010101000101001 0 - wiadomość

Blum-Blum-Shub

$$x_{n+1} = (x_n)^2 \mathrm{mod} M$$

$$M = xy$$

$$x \mathrm{mod} 4 = 3$$

$$y \mathrm{mod} 4 = 3$$

$$\mathrm{NWD}(\phi(x-1), \phi(y-1)) <\text{- „małe”}$$

Szyfry asymetryczne

- 2 klucze (publiczny i prywatny)
- bazują na „trudnych” problemach matematycznych
- stosowane do podpisów cyfrowych
- inicjuje się nimi bezpieczną komunikację

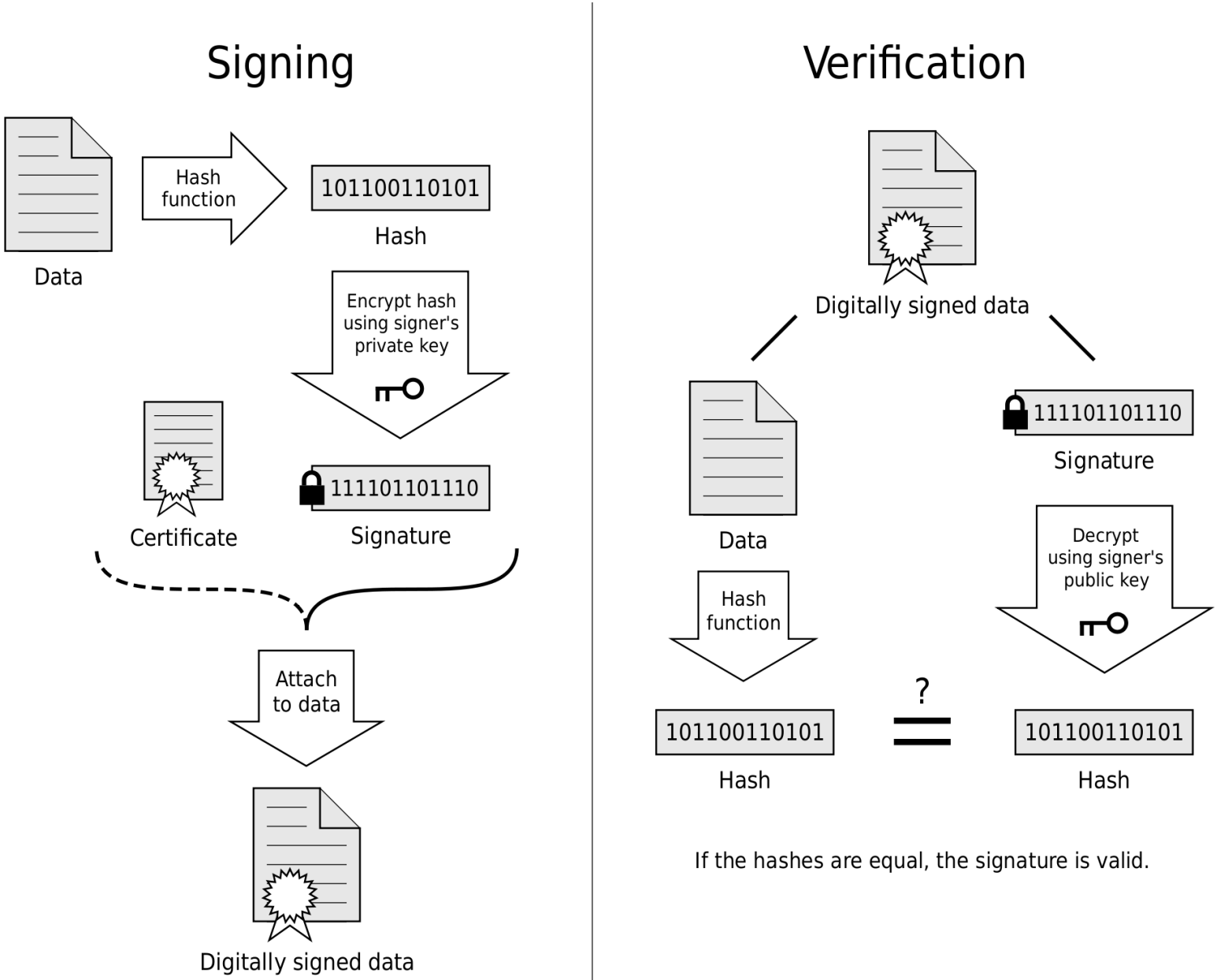
Zastosowania

Przeglądarki

HTTP**S**://....

1. Szyfrowane połączenie (SSL/TLS)
2. Zabezpieczenie certyfikatem

Podpis cyfrowy



Szyfrowanie plików

OpenSSL - szyfrowanie

```
$ openssl enc -aes-128-cbc -in sintel-1024-stereo.ogv
-out sintel-1024-stereo.ogv.aes
```

OpenSSL - deszyfrowanie

```
$ openssl enc -d -aes-128-cbc -in
sintel-1024-stereo.ogv.aes -out
sintel-1024-stereo.ogv.two
```

Szyfrowanie partycji

Propozycje (OpenSource)

- Linux Unified Key Setup
- TrueCrypt