EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kryptologie

Moderní kryptologie: Úvod

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

Doc. Ing. Roman Šenkeřík, Ph.D. FAI,
Ústav informatiky a umělé inteligence

Obsah prezentace

- Moderní kryptologie
  - Úvod
  - Matematické základy
- Vernamova šifra
  - Klasická verze
  - One-time-pad
- Symetrické blokové a proudové šifry
  - Základní schémata a přehled nejpoužívanějších algoritmů
  - Proudové šifry – rozdělení, inicializace, aplikace

1. Úvod do moderní kryptologie

Moderní kryptologie: Úvod

- Za přechod mezi klasickou a moderní kryptografii lze považovat následující milníky:

- 1917: Gilbert Vernam – objev Vernamovy šifry (upravená polyalfabetická šifra) patentována “nová” proudová šifra, později upravena do podoby známé jako “One-time Pad.

- 1948: Claude Elwood Shannon definoval zlom v historii kryptografie: Síla algoritmu má spočívat na pilířích matematické složitosti a ne na tajnostech kolem něj.

Moderní kryptologie: Matematické základy

Moderní kryptologie je postavena zejména na extrémní algoritmické složitosti výpočtu a analýzy klíčového prostoru. Využívá se zde řady principů a teorií [1]:

- Teorie přirozených čísel a prvočísel.
- Základní věty aritmetiky.
- Fermatovy věty.
- Eulerovy funkce.
- Diskrétního logaritmu.

2. Vernamova šifra

Vernamova šifra – Klasická verze

Spočívá v posunu každého znaku zprávy o náhodně zvolený počet míst v abecedě. To se prakticky rovná náhradě zcela náhodným písmenem a na tomto faktu je založen důkaz, že Vernamova šifra je v principu nerozluštitelná.

- V podstatě se jedná o Vigenerovu šifru s náhodným klíčem, případně Autokláv, kde startup klíč je ve své podstatě stejně dlouhý jako text.
- Opět platí jednoduchý matematický vztah pro šifrování:
- (Znak + klíč) mod 26

Vernamova Šifra – Klasická verze

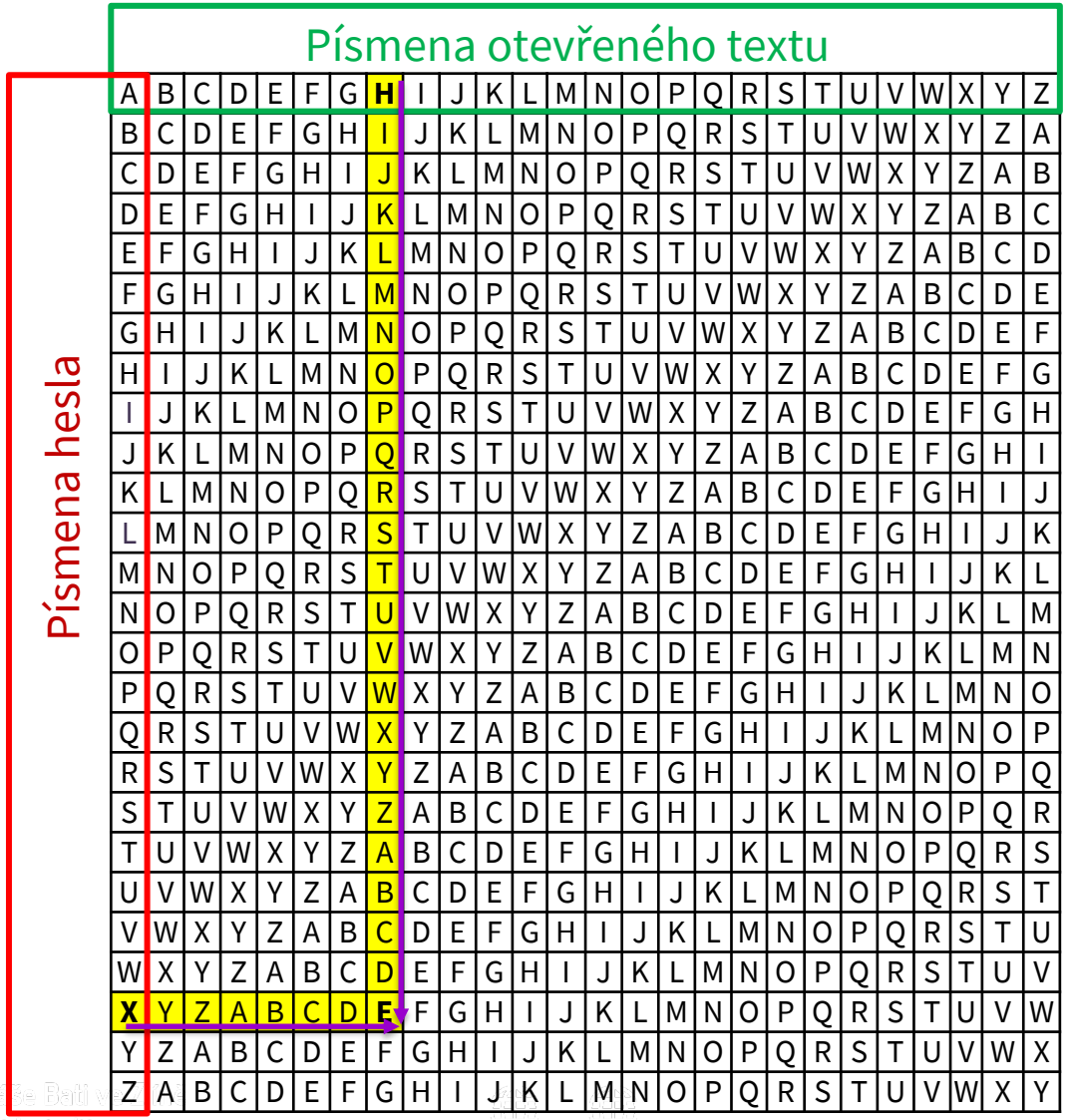
Šifrování

		H		E		L		L		O	message
	7	(H)	4	(E)	11	(L)	11	(L)	14	(O)	message
+	23	(X)	12	(M)	2	(C)	10	(K)	11	(L)	key
=	30		16		13		21		25		message + key
=	4	(E)	16	(Q)	13	(N)	21	(V)	25	(Z)	message + key (mod 26)
		E		Q		N		V		Z	ciphertext

Dešifrování

		E		Q		N		V		Z	ciphertext
	7	(E)	16	(Q)	13	(N)	21	(V)	25	(Z)	ciphertext
-	23	(X)	12	(M)	2	(C)	10	(K)	11	(L)	key
=	-19		4		11		11		14		ciphertext - key
=	7	(H)	4	(E)	11	(L)	11	(L)	14	(O)	ciphertext - key (mod 26)
		H		E		L		L		O	messange

Příklad dle: [2]



Doc. Ing. Roman Šenkeřík, Ph.D. FAI,
Ústav informatiky a umělé inteligence

Vernamova šifra – One-time pad

- První patentovaný koncept proudové šifry, tedy jednoduché binární operace mezi daty a klíčem (pad).
- Výhoda - stejný algoritmus je možné použít pro zašifrování i dešifrování
- Velmi “velký” klíč je běžně nenápadně přenášen pomocí zdánlivě neškodných médií a zařízení

Zdroj: [2]

Vernamova šifra – One-time pad

- Operace XOR mezi náhodným klíčem s normálním rozložením a stejnou délkou jako ŠT.

```
SENDING
-------------
message:    0 0 1 0 1 1 0 1 0 1 1 1 ...
pad:        1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR         -------------------------------
cipher:     1 0 1 1 0 0 0 1 1 1 0 0 ...

RECEIVING
-----------------
cipher:     1 0 1 1 0 0 0 1 1 1 0 0 ...
pad:        1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR         -------------------------------
message:    0 0 1 0 1 1 0 1 0 1 1 1 ...
```

Příklad dle: [3]

Pravdivostní tabulka XOR

VSTUPY		VÝSTUP
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Vlastnosti Vernamovy šifry

- **Klíč je tak dlouhý jako přenášená zpráva.** Jiné šifrovací systémy používají kratší klíče. Kratší klíč v principu umožňuje útok hrubou silou.

- **Klíč je dokonale náhodný.** Nepřipadají v úvahu počítačové generátory pseudonáhodných čísel, neboť jejich činnost lze poměrně snadno předvídat. Nejvhodnější je užití fyzikálních metod, například tepelného šumu či ještě lépe kvantových procesů, jejichž základní vlastností je náhodnost.

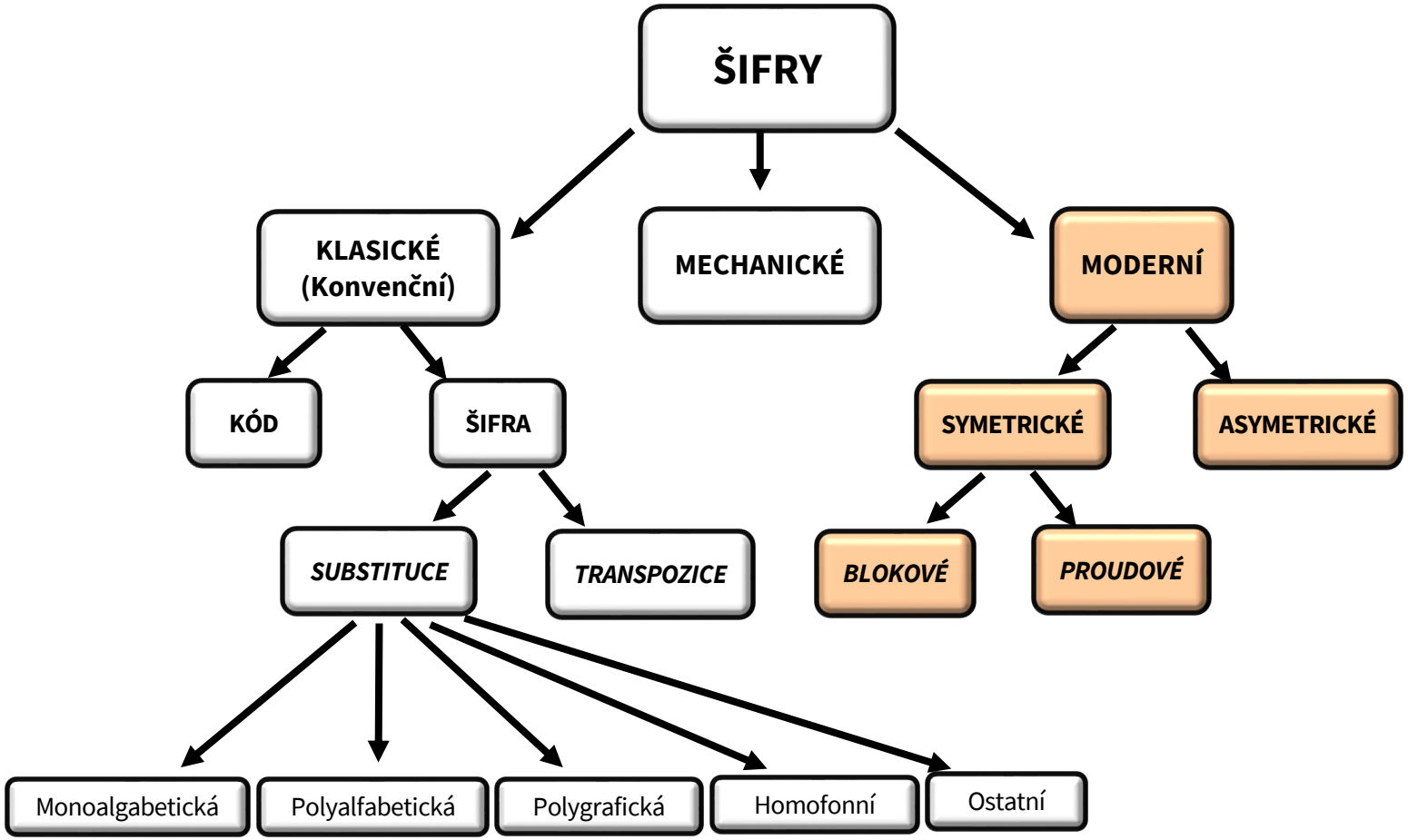
- **Klíč nelze použít opakovaně.** Tato podmínka je vlastně důsledkem předchozí, protože opakovaný klíč není náhodný. Dostane-li útočník do ruky dvě zprávy zašifrované týmž klíčem, má často velmi snadnou cestu k rozluštění.

Vlastnosti Vernamovy šifry

- **Statistická kryptoanalýza je znemožněna** náhodným charakterem šifrového textu. Nelze z něj zjistit žádné informace o četnosti znaků v původní zprávě ani vztahy mezi skupinami znaků apod.

- **Ani útok hrubou silou**, vůči kterému není odolná prakticky žádná jiná šifra, neuspěje. I kdyby měl útočník k dispozici neomezený výpočetní výkon, kvantové počítače a podobně a mohl systematicky vyzkoušet všechny možné klíče délky n, pak výsledkem snažení bude pouze posloupnost všech možných zpráv délky n. Nebude schopen mezi nimi nalézt tu správnou, nezíská o ní žádnou informaci. Ani pořadí, v jakém zprávy získal, neřekne útočníkovi nic, neboť za předpokladu náhodné volby klíče je také zcela náhodné.

Rozdělení moderních šifer



Příklady moderních šifer

- Neprolomitelná Vernamova šifra (One time pad)
- Symetrické proudové šifry - FISH, RC4
- Symetrické blokové šifry - DES, Tripple DES, AES, IDEA, CAST, BLOWFISH
- Asymetrické šifry (s veřejným klíčem) – RSA, ElGamal
- Asymetrické protokoly – Diffie Helman
- Hybridní šifry - PGP
- DSS - Digital Signature Standard, DSA - Digital Signature Algorithm
- ECDSA - DSA založené na standardu Eliptických křivek
- ...
- HASH funkce
- Kvantové šifrování, Teorie Chaosu, Fraktální a Neuro-Fraktální šifry

3. Symetrické blokové a proudové šifry

Symetrické proudové šifry

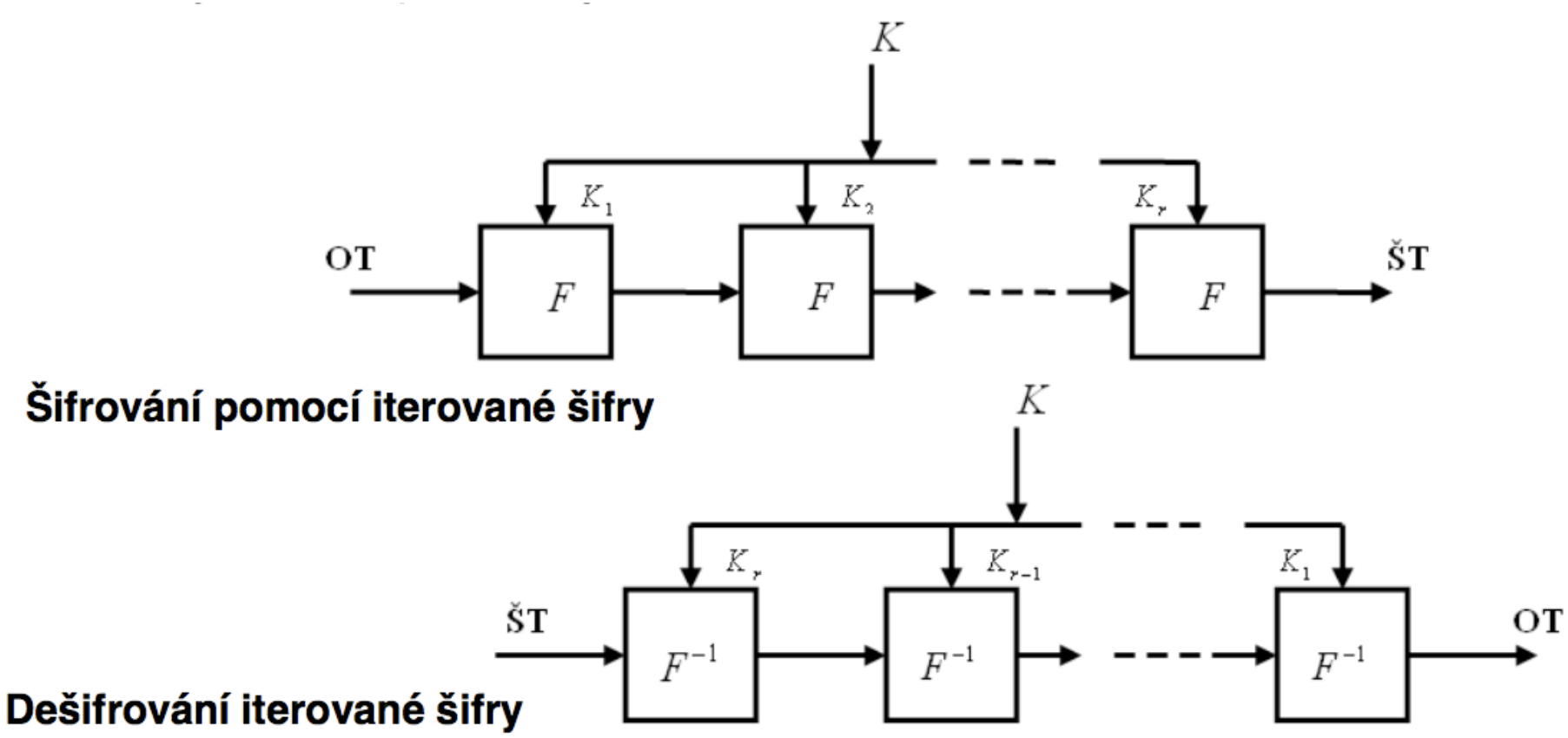
- Proudové šifry zpracovávají otevřený text po jednotlivých bitech.
- Inspirace zejména u Vernamovy šifry.
- Odlišují se především způsobem generování klíče.
- Namísto náhodné sekvence se OT kombinuje pomocí operace XOR s pseudonáhodnou sekvencí klíče.
- Synchronní varianta - klíč je generován nezávisle na OT.
- Samo-Synchronizační varianta - využívá vždy několik bytů z ŠT (využití zpětné vazby).
- Nejznámější: RC4, FISH, A5/1, A5/2, HELIX, CHAMELEON, ...

Symetrické blokové šifry

Blokové šifry rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost

- ŠT se získává z OT nejčastěji pomocí opakované rundové funkce (iterační proces).
- OT i ŠT mají pevnou délku.
- Vstupem do rundové funkce je klíč a výstup z předchozí rundy (iterace).

Blokové šifry - schéma



Zdroj: [4]

Feistelova Struktura (síť)

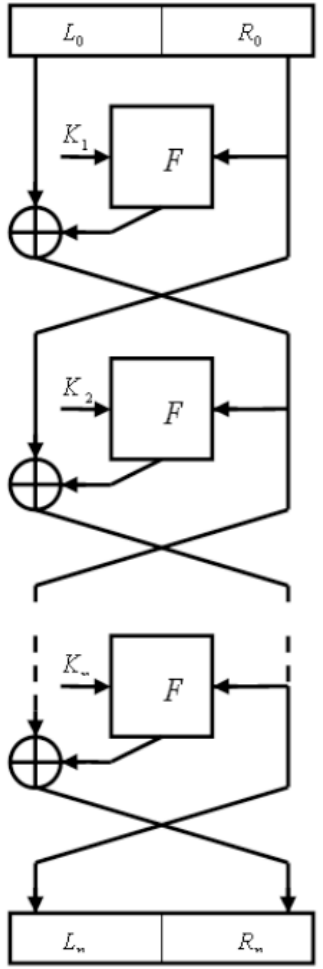
- Velké množství symetrických blokových šifer využívá tzv Feistelovu strukturu (síť).

- Feistelova šifra představuje určitý způsob zpracování dat v šifrovacích systémech a nikoliv konkrétní algoritmus

Feistelova Struktura (síť)

Základní princip: Dělení OT na dvě poloviny.

V další iteraci se pravá část OT stává levou a původní levá čast je zpracována přes tzv. rundovou (Feistelovu) funkci s využitím podklíče.



Zdroj: [4]

Doplněk k moderním symetrickým šifrám

- **U moderních symetrických šifer** vyvstal problém, jak zajistit v praxi základní kryptografické pravidlo, tak, aby dva texty (data), ale zejména stejné texty (data) byla vždy šifrována různým klíčem.

- **U proudových šifer** se jedná o kritický prvek - šifrování WiFi provozu, datastreamů používá často stejný klíč nastavený na hodiny, dny, roky dopředu. Na základě tohoto klíče se generuje dostatečně dlouhý keystream (klíč) pro pokrytí provozu šifry. Je nutné do tohoto procesu vnést stochastický prvek - náhodný nebo pseudonáhodný *inicializační vektor* (IV). Pomocí něj a klíče se generuje provozní klíč šifry - zajištění různého výstupu pro stejný klíč a vstupní data.

Doplněk k moderním symetrickým šifrám

- **U blokových šifer** problém vyvstává, pokud jsou data k zašifrování větší než dělka bloku. Docházelo by k situacím, kdy by různé po sobě jdoucí bloky byly šifrovány vždy stejným klíčem (stejnou sadou rundových podklíčů). Proto u blokových šifer byl standardizován tzv. *režim činnosti*, který popisuje, jakým způsobem se šifrují data o větším objemu dat, než je velikost bloku a jakým způsobem se operuje zde s tzv. *inicializačním vektorem*.

Seznam odkazů

[1] ZEMAN, Václav, Zdeněk Martinásek. Kryptografie v Informatice. VUT v Brně, 2014.

[2] One-time pad. [online]. Dostupné z: https://en.wikipedia.org/wiki/One-time_pad

[3] WHITMAN, Michael E. a Herbert J. MATTORD. Principles of Information Security. 3rd ed. Boston: Thomson Course Technology, [2008]. ISBN 1-4239-0177-0.

[4] Moderní blokové šifry I. Tomáš Vaněk. [online]. Dostupné z: rantos.cz/IBE-prezentace/P03_Blokove_sifry_v1.4.3SHORT.pdf

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204