Hesla a bezpečnost na internetu

MjUNI 2019

Dětská univerzita, 13. 4. 2019

Vladimír Sedláček, vlada.sedlacek@mail.muni.cz

Marek Sýs, syso@mail.muni.cz

CROCS

Centre for Research on Cryptography and Security

Osnova

Hesla:

- Jaké jsou typické problémy?
- Jak si zvolit silné heslo?
- Jaké jsou dobré praktiky, kterými se řídit?

Osnova

Hesla:

- Jaké jsou typické problémy?
- Jak si zvolit silné heslo?
- Jaké jsou dobré praktiky, kterými se řídit?

Bezpečnost:

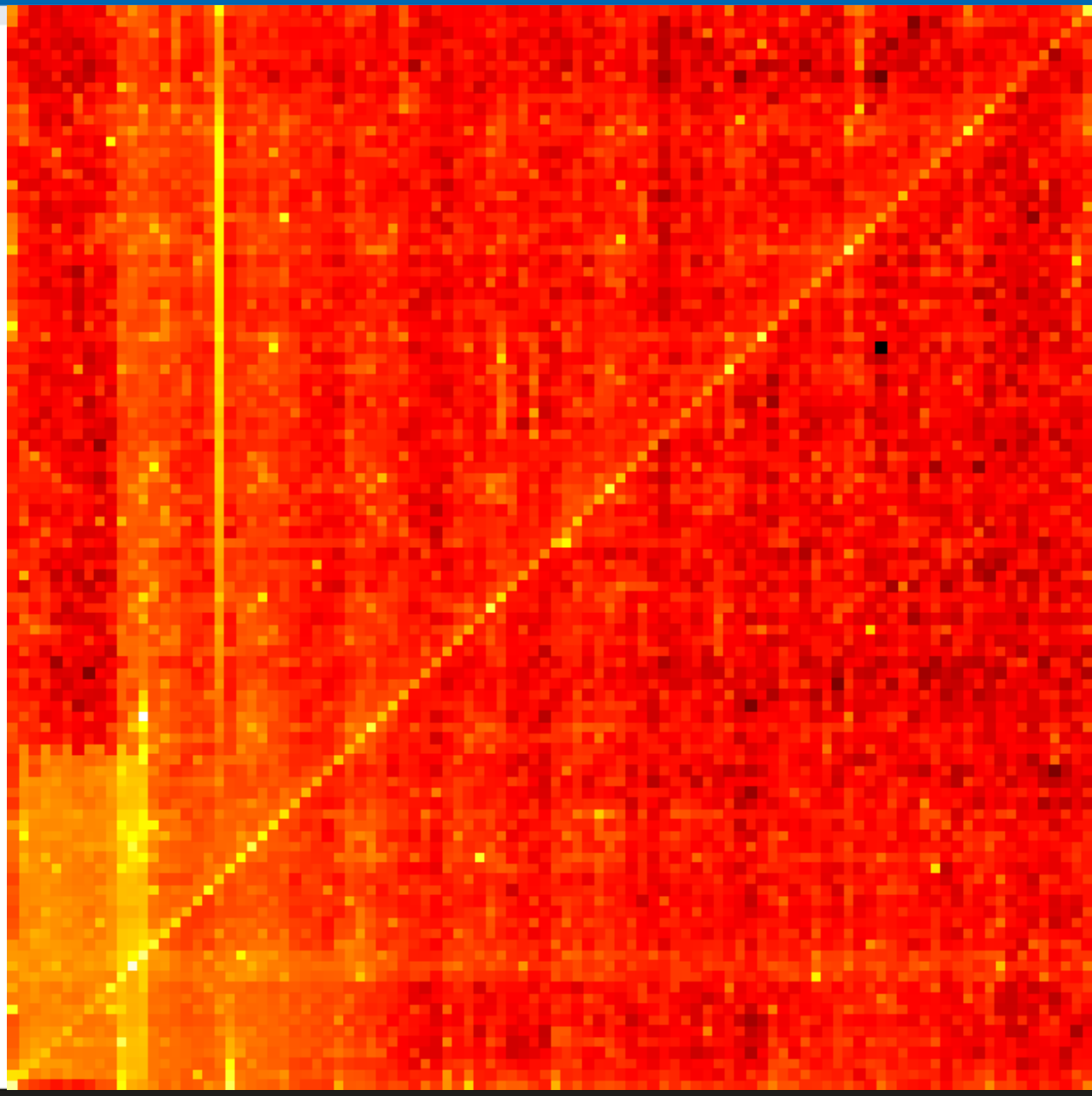
- Co je šifrování a kde se používá?
- Co jsou elektronické podpisy?
- Proč si Slováci museli vyměnit občanky?

PIN kódy

- Jaké PIN kódy lidé používají?
- Dataset 3.4 milionů 4-místných PINů a hesel (0000-9999)

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

Frekvence PIN kódů



Útok hrubou silou

Heslo tvoří	Počet znaků	Délka hesla								
		2	3	4	5	6	7	8	9	10
jen čísla	10	hned	hned	hned	hned	hned	1s	10s	1m40s	17m
jen malá nebo jen velká písmena	26	hned	hned	hned	1s	31s	13m	6h	6d	163d
jen malá nebo jen velká písmena a čísla	36	hned	hned	hned	6s	4m	2h	3d	118d	12r
malá i velká písmena	52	hned	hned	1s	38s	33m	1d5h	62d	9r	458r
malá i velká písmena a čísla	62	hned	hned	2s	2m	1h35m	4d	253d	43r	2661r
malá i velká písmena a speciální znaky	85	hned	hned	5s	7m24s	10h	37d	9r	734r	62428r
malá i velká písmena, čísla a speciální znaky	95	hned	hned	8s	13m	20h	81d	21r	1999r	189858r

1391 uniklých českých účtů

coufalova.veronika@gmail.com	vyhrajuto
katerina.blahova98@seznam.cz	komunikace
vanzura.honza@gmail.com	honza
zdendasmrha@seznam.cz	735038962
101520@seznam.cz	102030
13.10.2000JANA@seznam.cz	ome642
1998markytka@seznam.cz	markytka1998
1istvik@seznam.cz	prdelka123
24ik@seznam.cz	
30anna@seznam.cz	3041998
585411053@iol.cz	sigmaolomouc
69.martina@seznam.cz	kyticka3
732598144@seznam.cz	hovnokleslo1
7wp54@seznam.cz	
8ann8@seznam.cz	080885
96kuby@seznam.cz	4komety
999patamat@gmail.com	bubu1970

adela.homutova@gmail.com	adelkabill
adelarumplikova@centrum.cz	ferdaapepa.1234
adelaryclova@seznam.cz	adelka1986
adelasvetnicka@seznam.cz	3799
adkar76@gmail.com	2256
adosbalos123@centrum.cz	
adulas110@gmail.com	nitro110
adynapavlicova@seznam.cz	
agnes.rap@seznam.cz	Heslo.124
agnesdedkova@gmail.com	jamakasi
Ajulinkadytrtova@seznam.cz	9453260289
ak.nah@seznam.cz	ga70ha
alaric2@seznam.cz	evenka
alca.babca@seznam.cz	masarinka
alena.slezakova@gmail.com	anarchy
alexandr.wojcik@seznam.cz	
alicekoblicova@seznam.cz	bobina1234

Home | Notify me | Domain search | Who's been pwned | Pastes | API | About | Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username | pwned?

181	2,050,475,902	43,342	39,995,452
pwned websites	pwned accounts	pastes	paste accounts

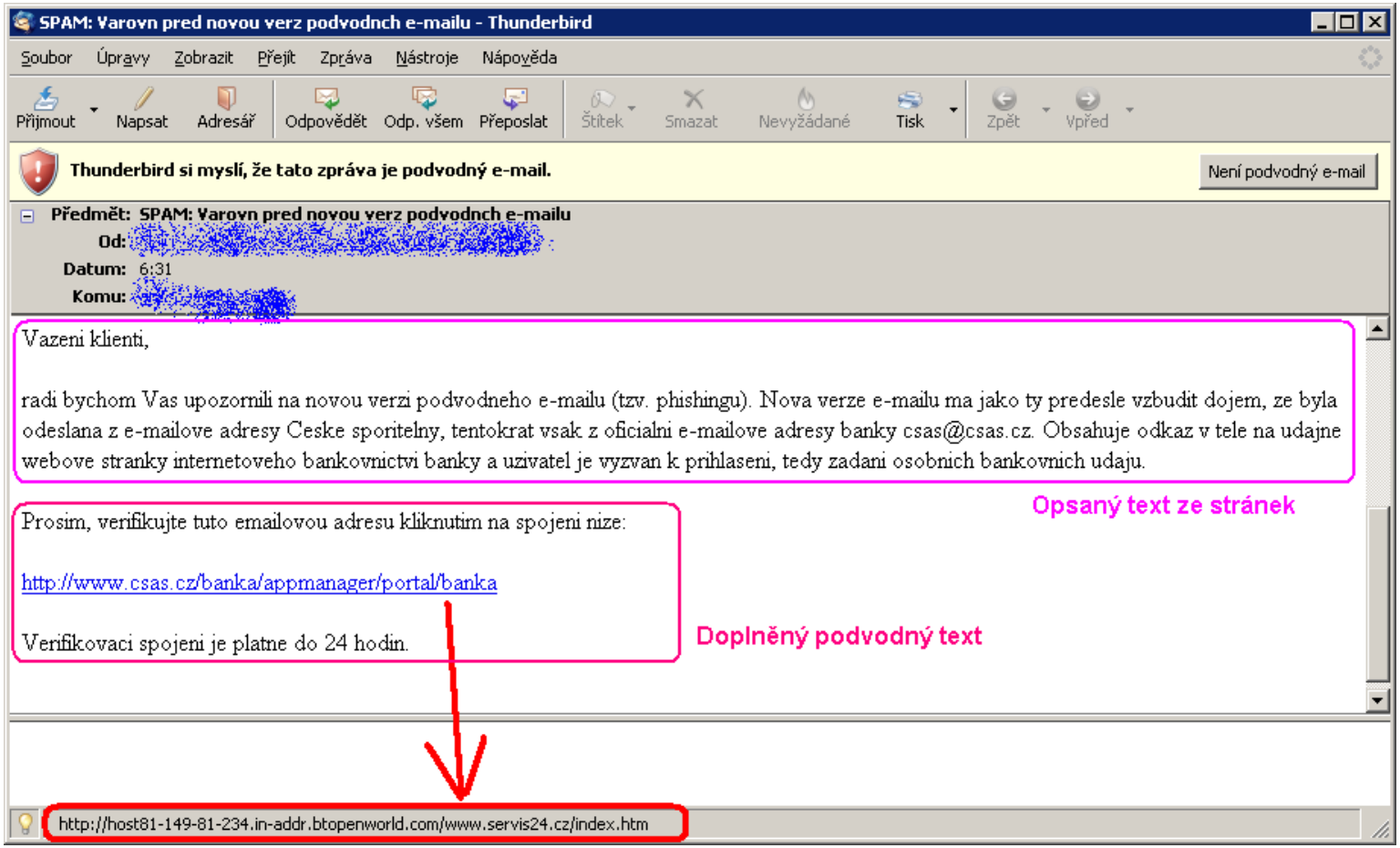
Top 10 breaches

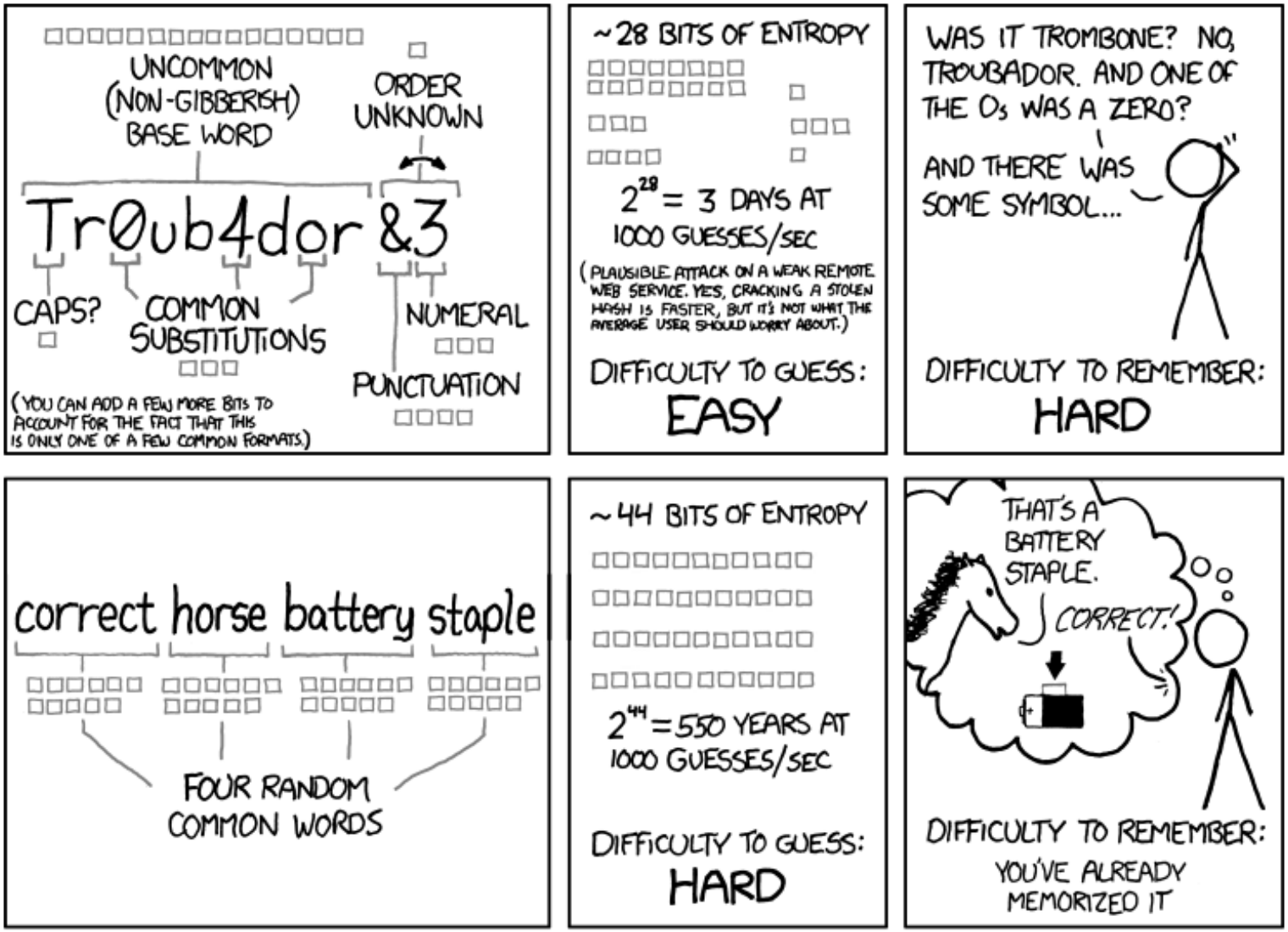
myspace	359,420,698	MySpace accounts
NetEase	234,842,089	NetEase accounts
in	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
badoo	112,005,531	Badoo accounts
	93,338,602	VK accounts
Рамблер/	91,436,280	Rambler accounts
	68,648,009	Dropbox accounts
tumblr.	65,469,298	tumblr accounts
	58,843,488	Modern Business Solutions accounts

Sociální inženýrství

https://www.youtube.com/watch?v=lc7scxvKQOo

Phishing


SPAM: Varovn pred novou verz podvodnch e-mailu - Thunderbird
Soubor Úpravy Zobrazit Přejít Zpráva Nástroje Nápověda
Přijmout Napsat Adresář Odpovědět Odp. všem Přeposlat Štítek Smazat Nevyžádané Tisk Zpět Vpřed
Thunderbird si myslí, že tato zpráva je podvodný e-mail.
Není podvodný e-mail
Předmět: SPAM: Varovn pred novou verz podvodnch e-mailu
Od:
Datum: 6:31
Komu:
Vazeni klienti,
radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu). Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Ceske sporitelny, tentokrat vsak z oficialni e-mailove adresy banky csas@csas.cz. Obsahuje odkaz v tele na udajne webove stranky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju.
Opsaný text ze stránek
Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize:
http://www.csas.cz/banka/appmanager/portal/banka
Verifikovaci spojeni je platne do 24 hodin.
Doplněný podvodný text
http://host81-149-81-234.in-addr.btopenworld.com/www.servis24.cz/index.htm

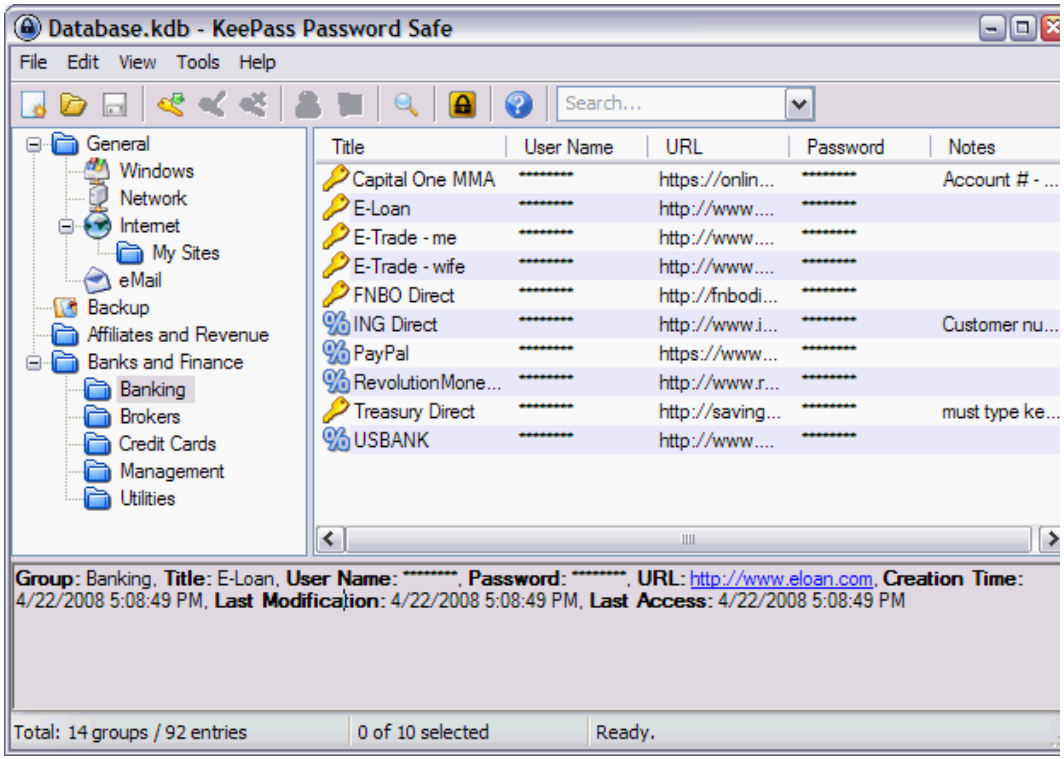


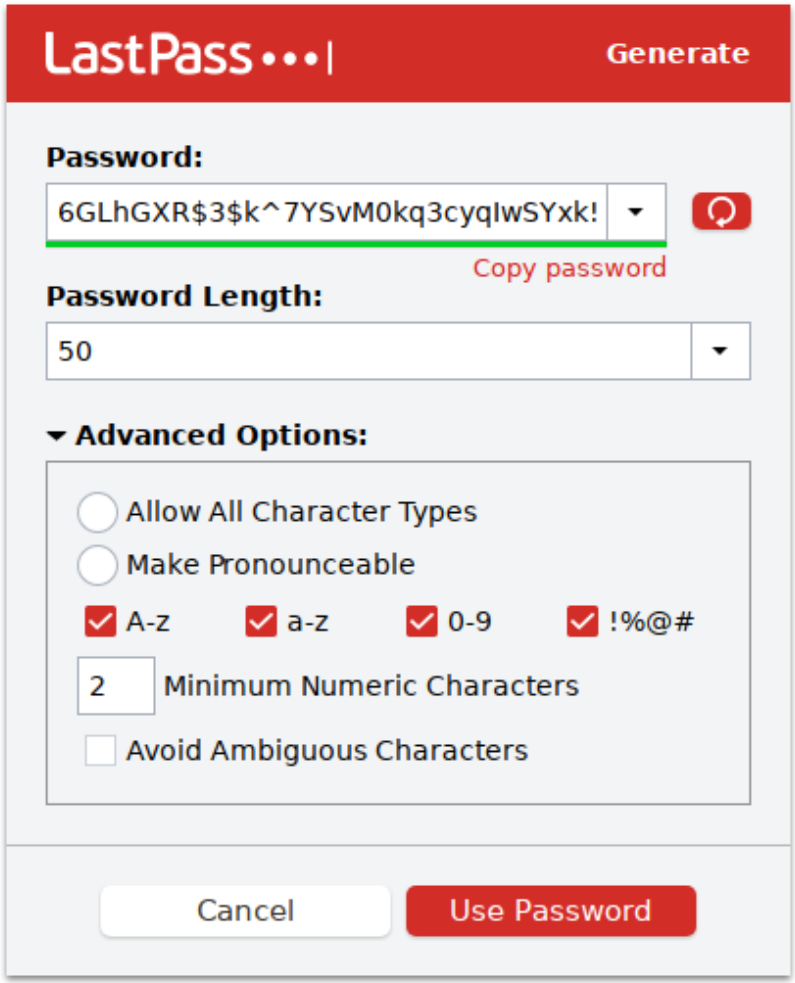
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Další metody tvorby hesel

- Hierarchie hesel dle důležitosti
- Password manager (např. LastPass, KeePass, 1Password)
- Slova/písmena z knih, citátů, přísloví, písní
- Mnemotechnické systémy (např. od Derrena Browna - Magie a manipulace mysli)
- Dvoufaktorová autentizace (2FA, např. Google Authenticator)

Password manager





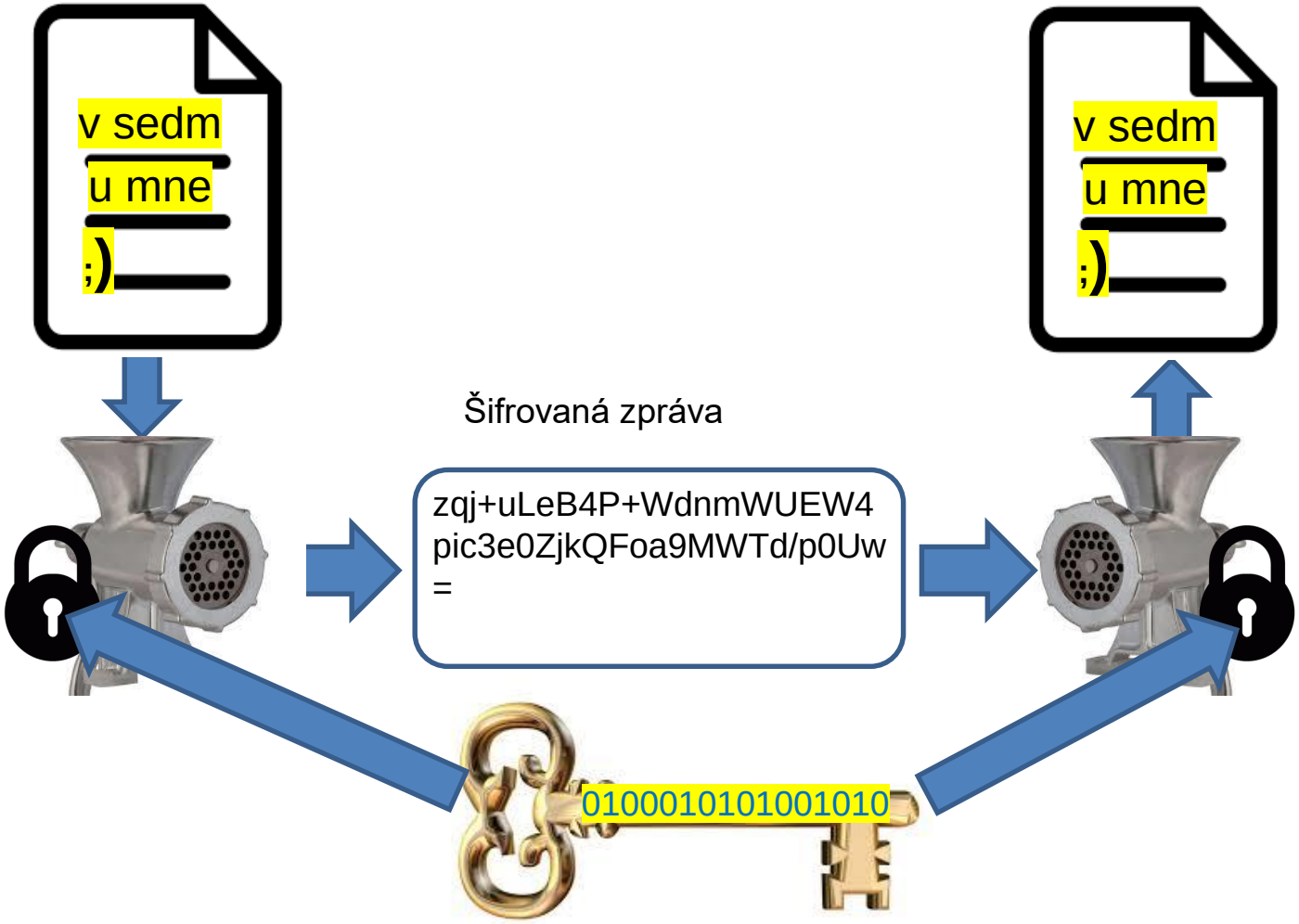
Hesla - co si odnést

- Slabá hesla a hesla použité na více stránkách mohou snadno uniknout
- Password manager a 2FA jsou velmi dobrou volbou
- Hesla rozhodně nechcete s nikým sdílet ani je zadávat na nezabezpečených stránkách / po vyzvání “autority”
- Kritické myšlení vás často může zachránit!

Šifrování

- Kde:
  - Manager hesel – databáze hesel
  - Internet – stránky (např. internet banking)
  - Komunikace s úřady – daňové přiznání, …
  - Hranice, letiště: elektronické občanky a pasy
- Na co:
  - Identifikace
  - Utajení dat
  - Elektronický podpis

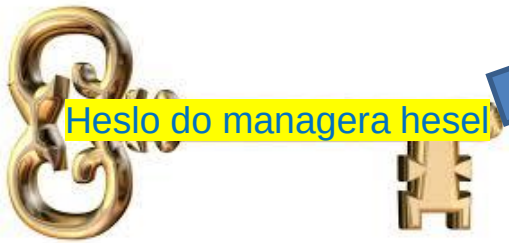
Klasické (symetrické) šifrování



Klasické šifrování

- Klíč + správa ⇒ šifra ⇒ zašifrovaná správa
  - klíč je **klíčový –** kdo ho zná muže šifrovat i dešifrovat

(např. hesla zašifrovaná osobním heslem v Keepass)



P8WL9FsxHLUzptfsU
gtcsAx…hiU…8tZ346
Fd7a…uKXPf…gqxC1
Y+Ss…7RPO
9t4A…qaZX
HN…74bYj
…7usvZ
0rkOD8rgN7luxMVID
GU9jRuQYGQ=

marek.sys@gmail.com mojeheslo1
marek.sys1@gmail.com mojeheslo1
sys@seznam.com mojeheslo2
sys1@seznam.com mojeheslo2

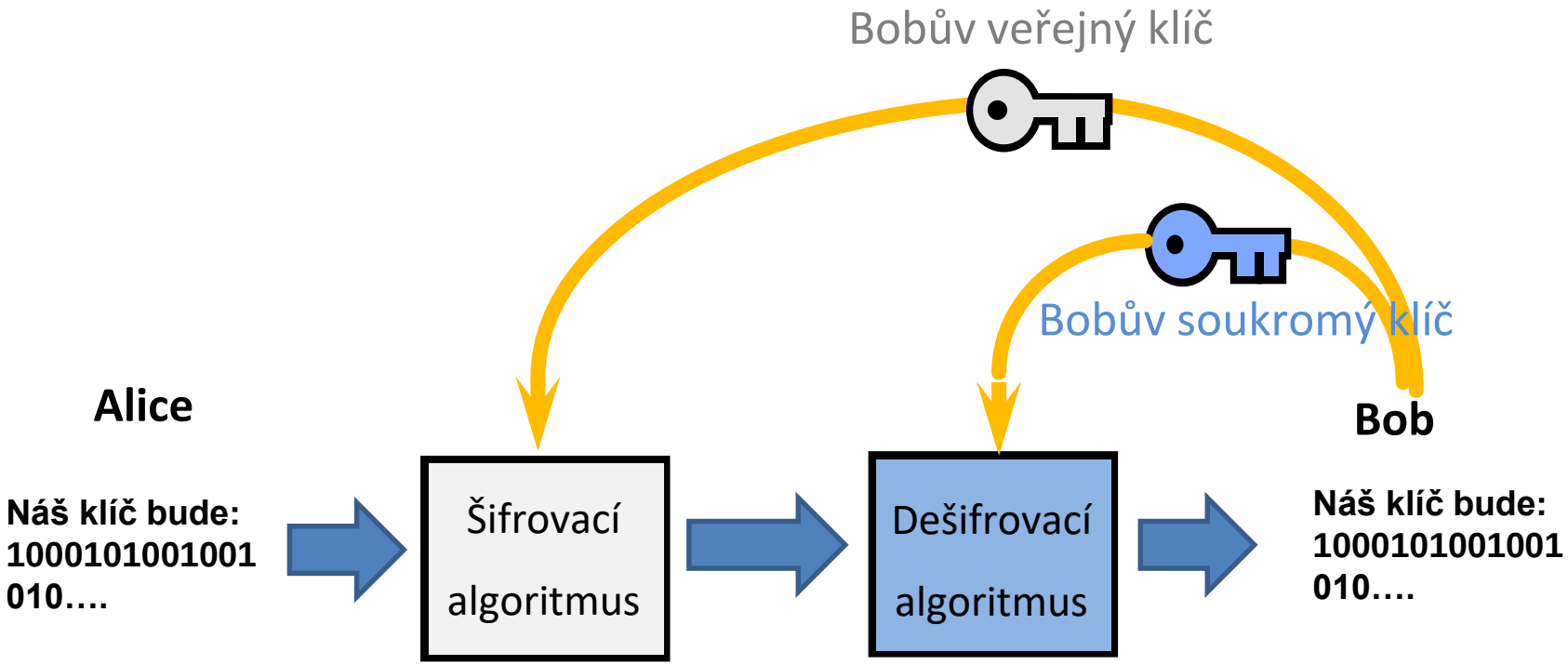
https://codebeautify.org/encrypt-decrypt

Internet není bezpečný

- Utajená komunikace – vyžaduje znalost klíče pro obě komunikující strany
- Jak se dohodnout na klíči když ...

Šifrování veřejným klíčem

Idea: 2 **různé** klíče (pro šifrování, pro dešifrování)



Převzato z: *Network and Internetwork Security* (Stallings)

Bezpečné stránky

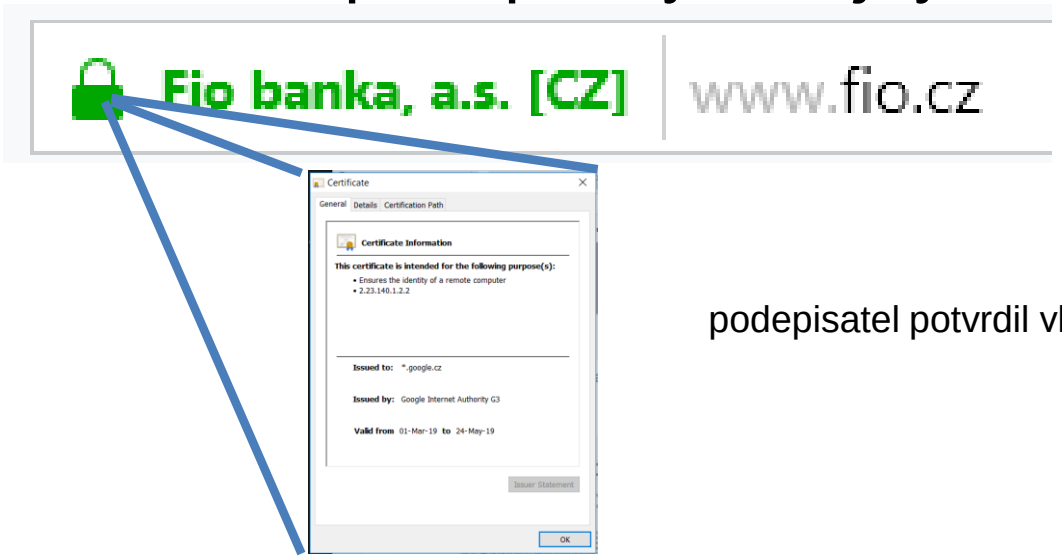
- Šifrované spojení

Certifikát

- Jak vím, že komunikuju s www.banka.cz

a ne s někým kdo se za banku vydává?

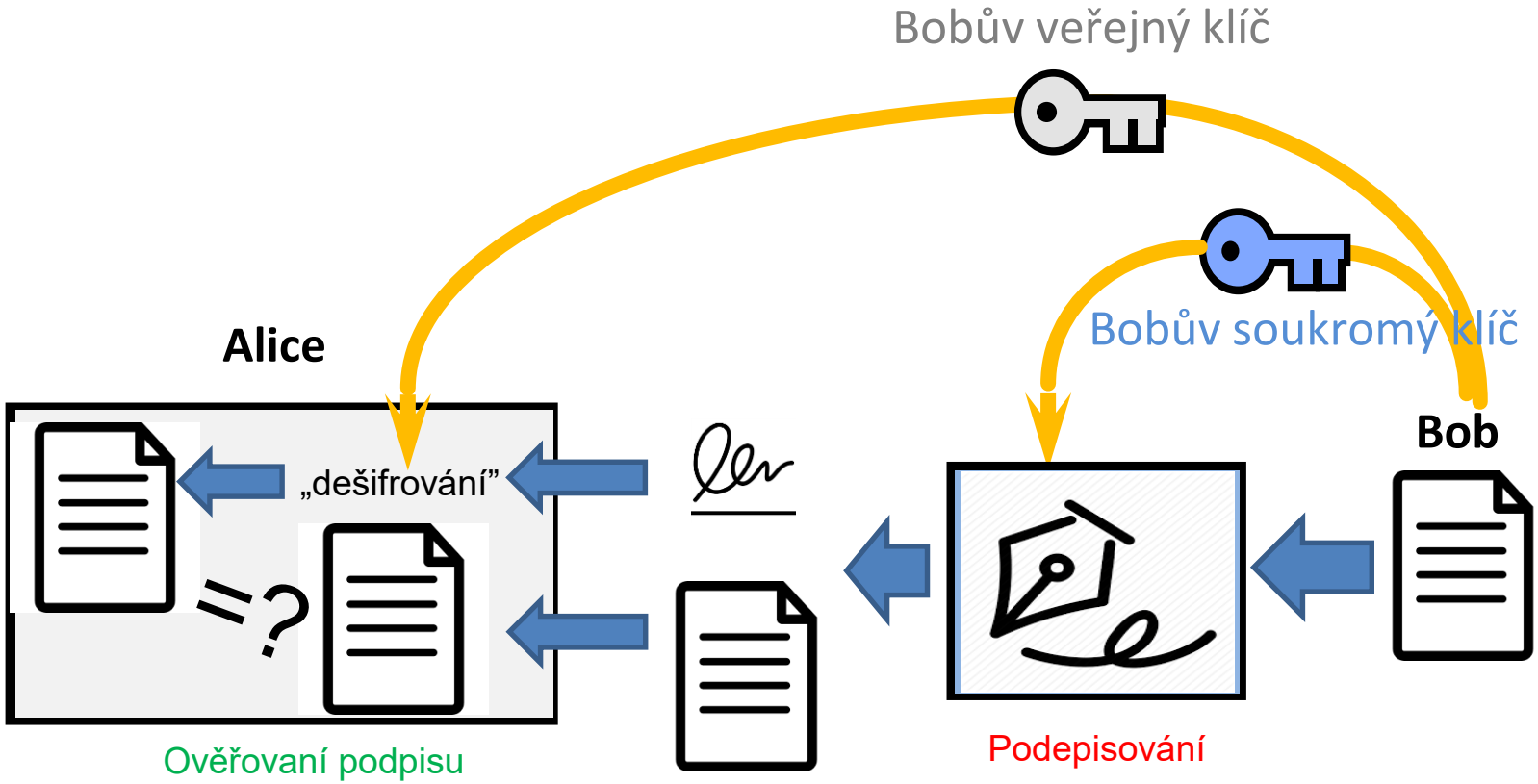
  - třeba zjistit, kdo je vlastník **veřejného** klíče!
- Certifikát = podepsaný veřejný klíč



podepisatel potvrdil vlastnictví klíče

Digitální podpis

- podobý princip jako při šifrování veřejným klíčem



Digitální podpis

- podepisuje se pomocí **soukromého** klíče
  - nikomu nedávat (nachází se napr. na čipu v el. občance https://info.eidentita.cz/eop/)
- ověřitelný (příslušným veřejným klíčem)
  - **kdokoliv** muže ověřit podpis
- Zabezpečuje:
  - nefalšovatelnost podepsaných dat(jinak nesedí podpis)
  - Identifikuje podepisatele (podpis pomocí el.občanky)

Kontrolní otázky

- Co potřebujete, aby ste mohli podepisovat daňové přiznání ?
  - soukromý klíč (na el. občance - nechte si jej aktivovat)
  - aplikaci na podepisování
- Co potřebuje daňový úřad na ověření?
  - certifikát (kvalifikovaný) s vašim veřejným klíčem

https://www.financnisprava.cz/cs/dane-elektronicky/danovy-portal/uznavany-elektronicky-podpis

Slovenské občanky

- problém specifických čipu
  - občanky Slovenska, Estonska, Španelska, ...
- nevhodne generované klíče výrobcem čipu
  - z veřejného klíče je možno spočítat soukromí klíč
- Slováci – zapíraní problému ... nakonec zneplatnení certifikátu ...