

Prezentace a linky



https://github.com/sysox/Mjuni_2025

Autentizace



MjUNI 2025 24.05.2025

Marek Sýs, syso@mail.muni.cz

Agáta Kružíková, kruzikova@mail.muni.cz

CRCS

Centre for Research on
Cryptography and Security

Osnova

- Úvod – autentizace
- Biometriky – falešný otisk
- Hesla – bezpečnost hesel, správce hesel
- Dvoufaktorová autentizace – hardware, software
- Komunikace a podpisy – certifikáty, el. podpisy

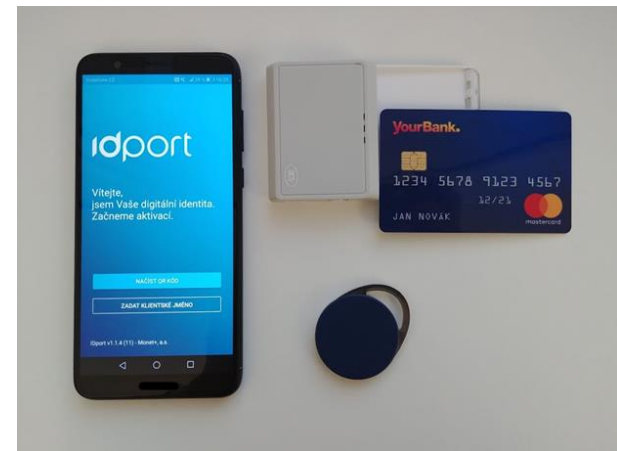
Autentizace

- Autentizace = Jak někdo prokáže, že je tím, za koho se vydává?
- Něco čím jsem
- Něco co mám
- Něco co znám

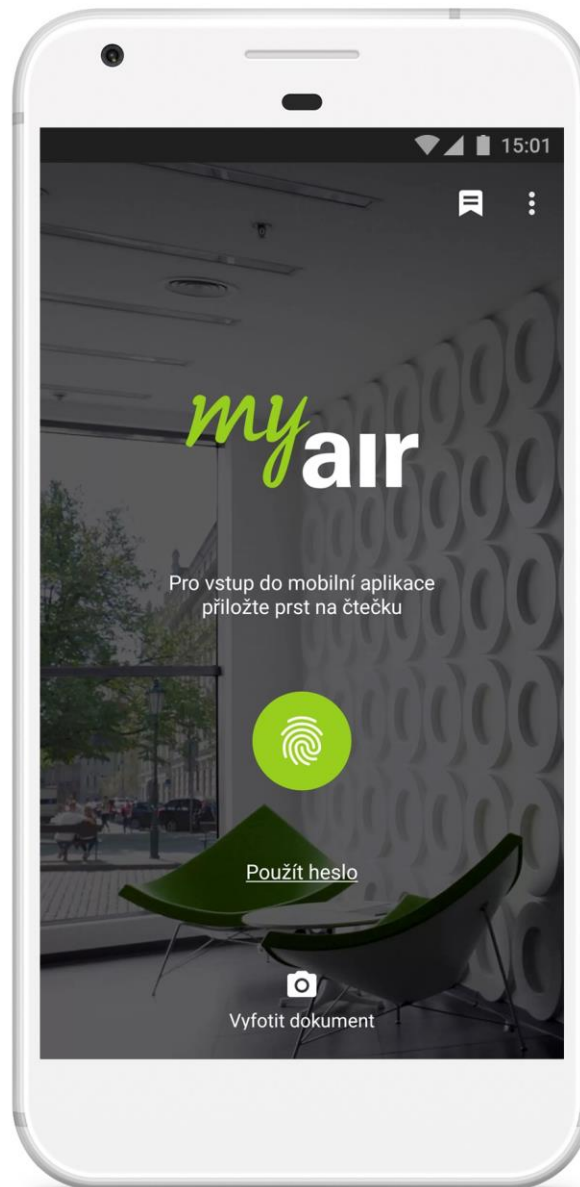
Autentizace

- Autentizace = Jak někdo prokáže, že je tím, za koho se vydává?

- Něco čím jsem
 - biometriky
- Něco co mám
 - bezpečnostní token,
 - chytrý telefon
- Něco co znám
 - heslo
 - šifrovací klíč

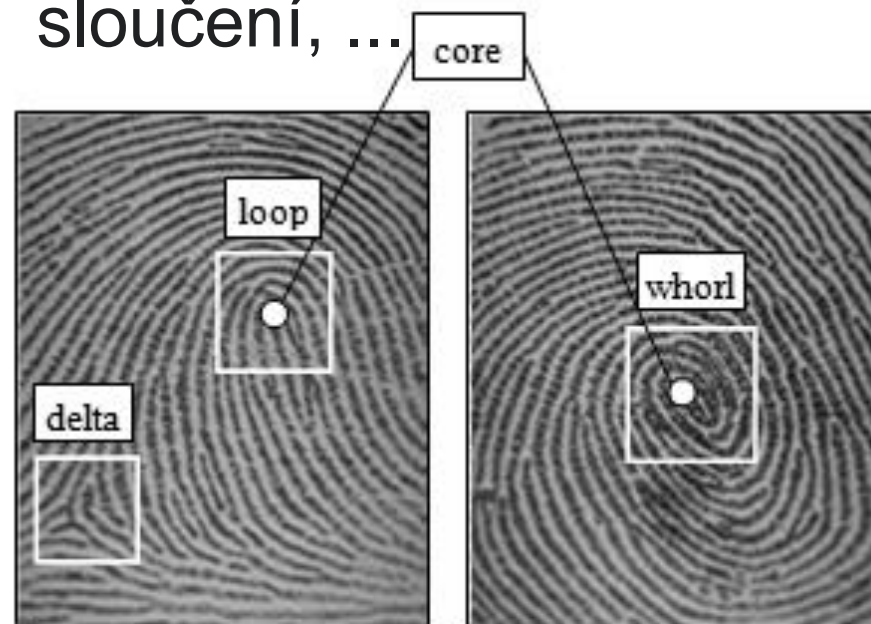
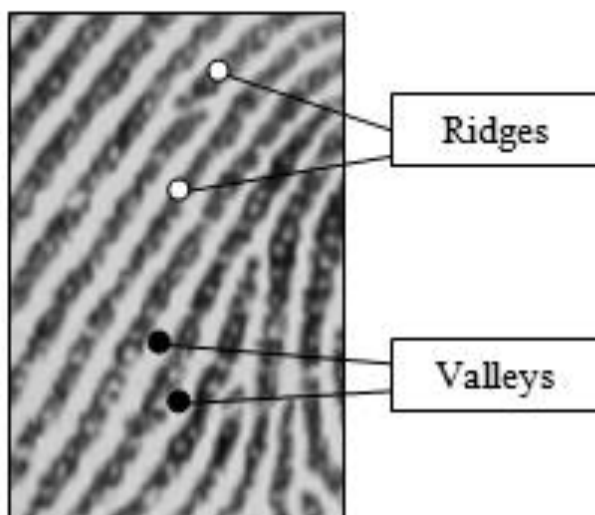


Biometriky



Otisk – z čeho se skládá

- Papilární linie = výběžky (oddělené údolím)
- Charakteristické znaky: **rozdvojení, ukončení, sloučení, ...**



Ukázka: čtečka + software



Otisk: mapa markantů

Biometric



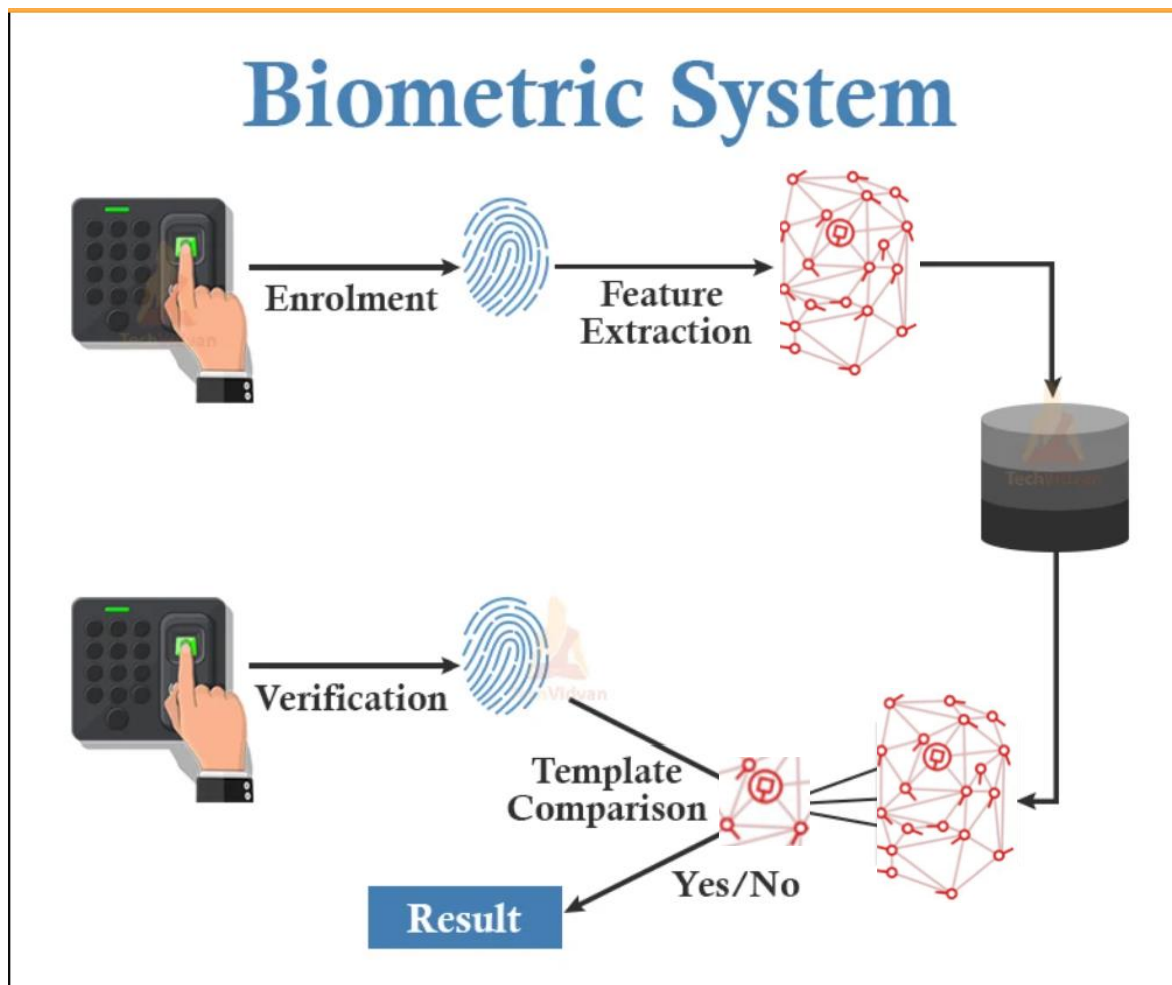
Minutia Points



Minutia Map



Autentizace pomocí otisku



Vytvoření falešného otisku

- S biometrikami opatrně!!
 - Nesdílet – nedají se změnit! 😊
- Scénáře jak získat otisk:
 1. Dobrovolně poskytnutý otisk
 2. **Nedobrovolně poskytnutý otisk – neetické!!**
 1. Fotka z internetu (např. TikTok)
 2. Fotka reálného otisku (povrch předmětu)

Dobrovolně poskytnutý otisk



Dobrovolně poskytnutý otisk - postup

1. Příprava plastelíny - hladký povrch
2. Otisk do plastelíny – přitlačit
3. Nalít výplň (cca vrstva 1.5 mm):
 - silikon (smíchaní 2 složek)
 - nebo lepidlo (Herkules), nebo želatina (Haribo), ...
4. Otisk:
 - schnutí (silikon cca 15 min.)
 - jemně odlepit

Nedobrovolně? poskytnutý otisk



Výzvy na sociálních sítích



Fotka z otisku na reálném povrchu

1. Zvýraznění pomocí jemného prachu (např. uhlíkový prášek) – prach přilne na mastnou část (otisk výběžků)



2. Vyfocení



Ukázka

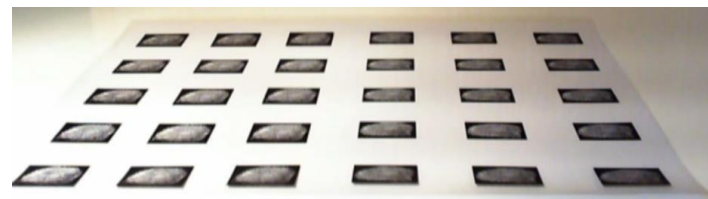
Předzpracování (např. GIMP)

- Fotka
- Změna barev na:
 - černo – bílá
 - bez odstínů šedi
- Vyčištění okolí otisku



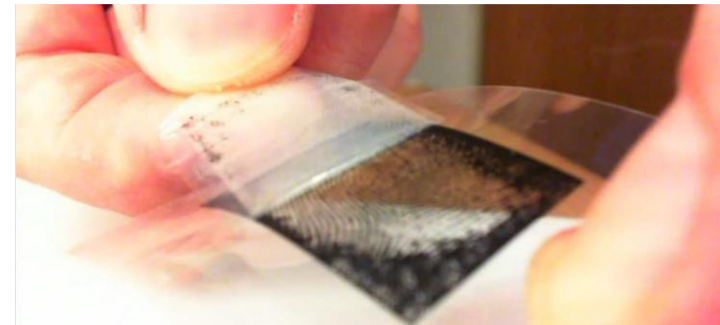
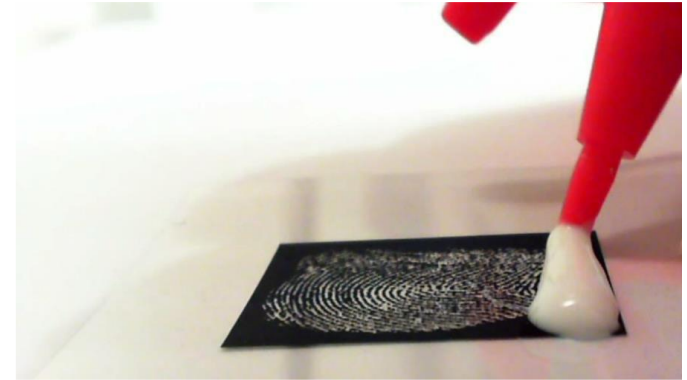
Falzifikace otisku I

- Předzpracovaný otisk
- Inverze barev
 - Bílá → černá
 - Černá → bílá
- Tisk na folii → 3D forma

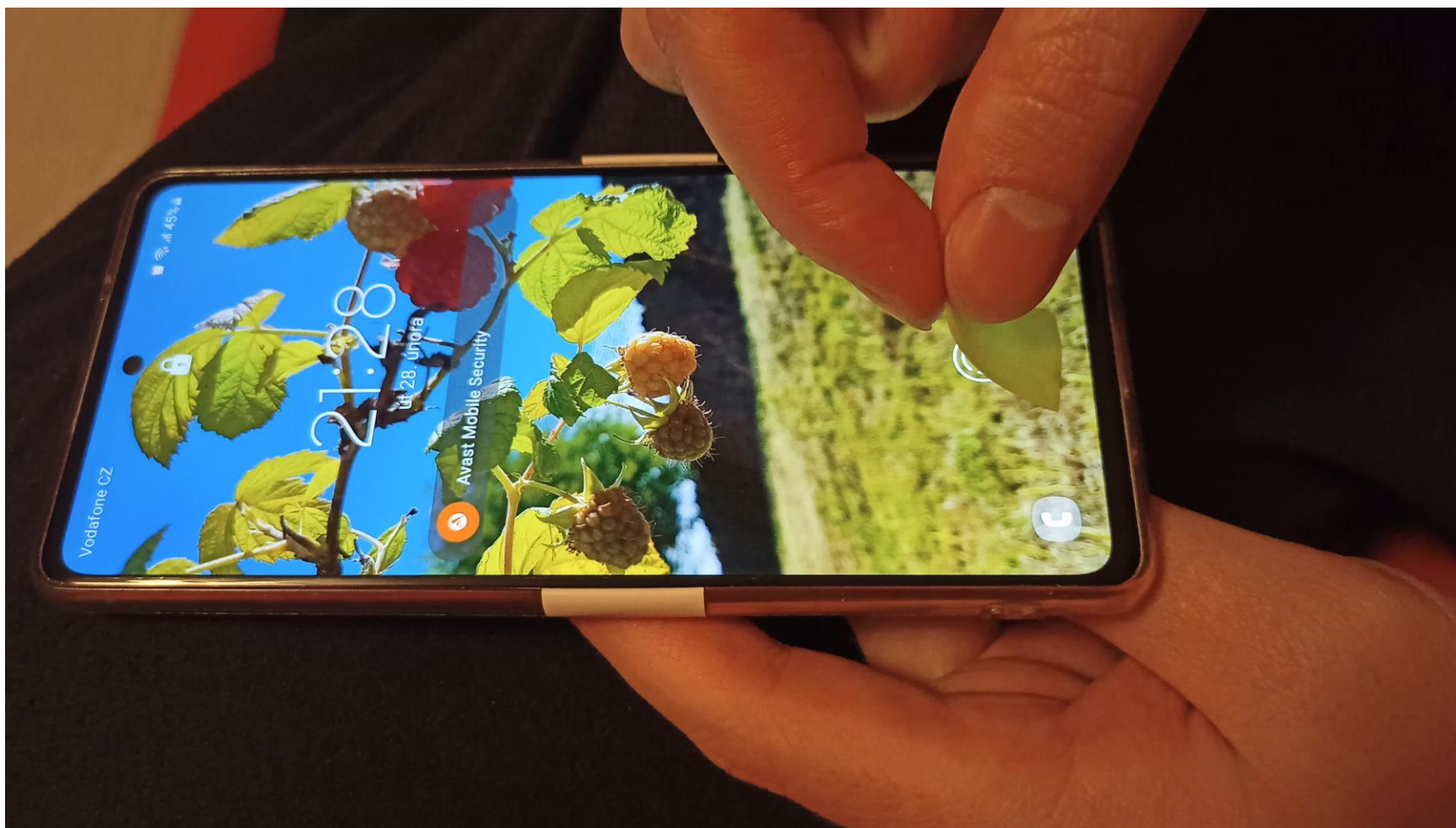


Falzifikace otisku II

- Nanesení lepidla (silikonu)
- Uschnutí (15 min) a sloupnutí
- Použití 😊



Ukázka



Hesla

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

..yy

0000

5555

xx..

9999

1391 uniklých českých účtů

coufalova.veronika@gmail.com	vyhrajuto	adela.homutova@gmail.com	adelkabill
katerina.blahova98@seznam.cz	komunikace	adelarumplikova@centrum.cz	ferdaapepa.1234
vanzura.honza@gmail.com	honza	adelaryclova@seznam.cz	adelka1986
zgendasmrha@seznam.cz	735038962	adelasvetnicka@seznam.cz	3799
101520@seznam.cz	102030	adkar76@gmail.com	2256
13.10.2000JANA@seznam.cz	ome642	adosbalos123@centrum.cz	
1998markytka@seznam.cz	markytka1998	adulas110@gmail.com	nitro110
1istvik@seznam.cz	prdelka123	adynapavlicova@seznam.cz	
24ik@seznam.cz		agnes.rap@seznam.cz	Heslo.124
30anna@seznam.cz	3041998	agnesdedkova@gmail.com	jamakasi
585411053@iol.cz	sigmaolomouc	Ajulinkadytrtova@seznam.cz	9453260289
69.martina@seznam.cz	kyticka3	ak.nah@seznam.cz	ga70ha
732598144@seznam.cz	hovnokleslo1	alaric2@seznam.cz	evenka
7wp54@seznam.cz		alca.babca@seznam.cz	masarinka
8ann8@seznam.cz	080885	alena.slezakova@gmail.com	anarchy
96kuby@seznam.cz	4komety	alexandr.wojcik@seznam.cz	
999patamat@gmail.com	bubu1970	alicekoblicova@seznam.cz	bobina1234



';--have i been pwned?

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

pwned?

181

pwned websites

2,050,475,902

pwned accounts











43,342

pastes

39,995,452

paste accounts

Top 10 breaches

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



SCAN ME



Ukázka

Útok hrubou silou

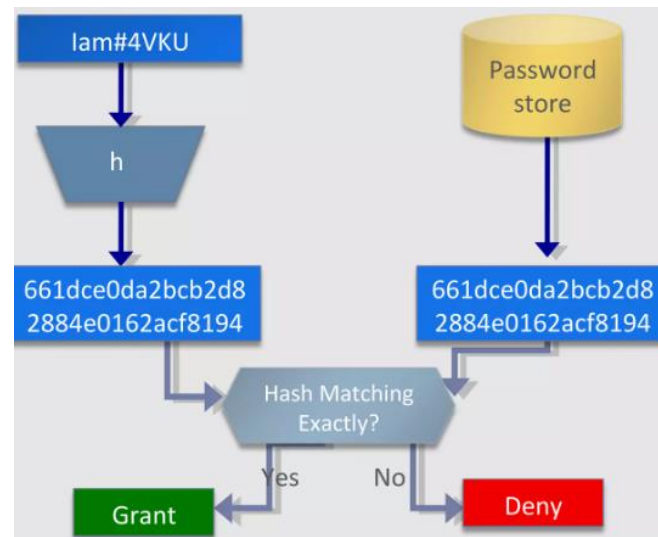
- Procházení všech možností:
 - aaaa, aaab, aaac, ...

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

Jak je uložené heslo

- Jako výsledek hashovací funkce
 - Nejde z něj heslo získat!
- Například: $\text{SHA1}(\text{'password'}) = 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8$

- Ověření:



Jak je uložené heslo

- Heslo není uloženo přímo, ale jako výsledek hashovací funkce! Nejde z něj heslo získat!
- $\text{SHA1}(\text{'password'}) =$
 $5\text{BAA}61\text{E}4\text{C}9\text{B}93\text{F}3\text{F}0682250\text{B}6\text{C}\text{F}8331\text{B}7\text{E}\text{E}68\text{F}\text{D}8$
- $\text{SHA1}(\text{password})$
 $= 5\text{BAA}61\dots$



Útok na hesla

- John-the-reaper - aplikace na lámání hesel
 - [Tutorial](#)
- Útok hrubou silou:
 - zkoušíme všechny možnosti hesel,
 - pro každý počítáme hash a testujeme jestli výsledek je v databázi.

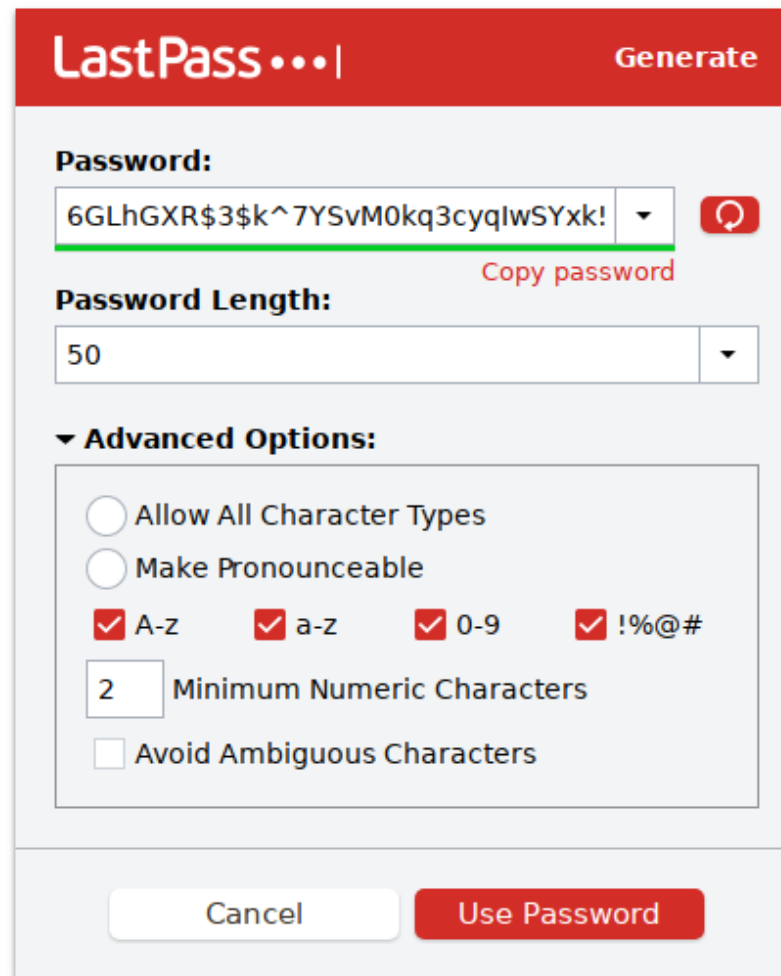
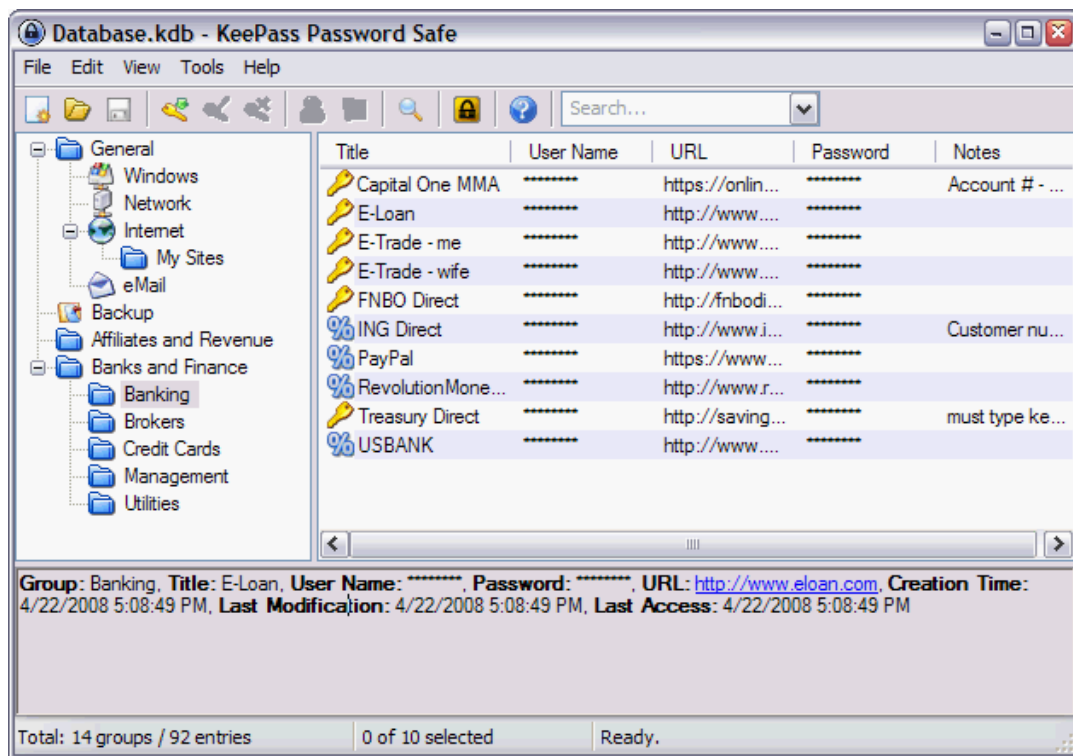


Ukázka

Správce hesel

Hlava není na hesla

Správci hesel do hloubky



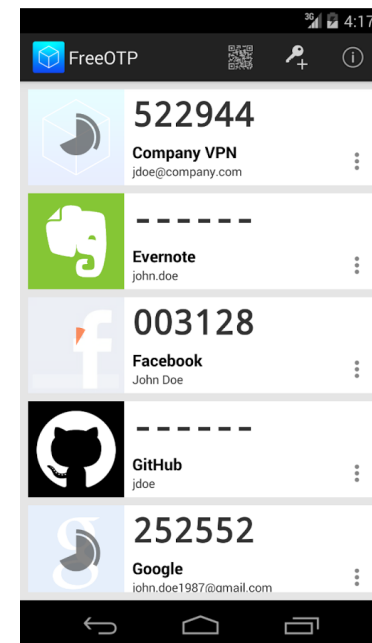
Dvoufaktorová autentizace

Dvoufaktorová autentizace ([2FA](#)):

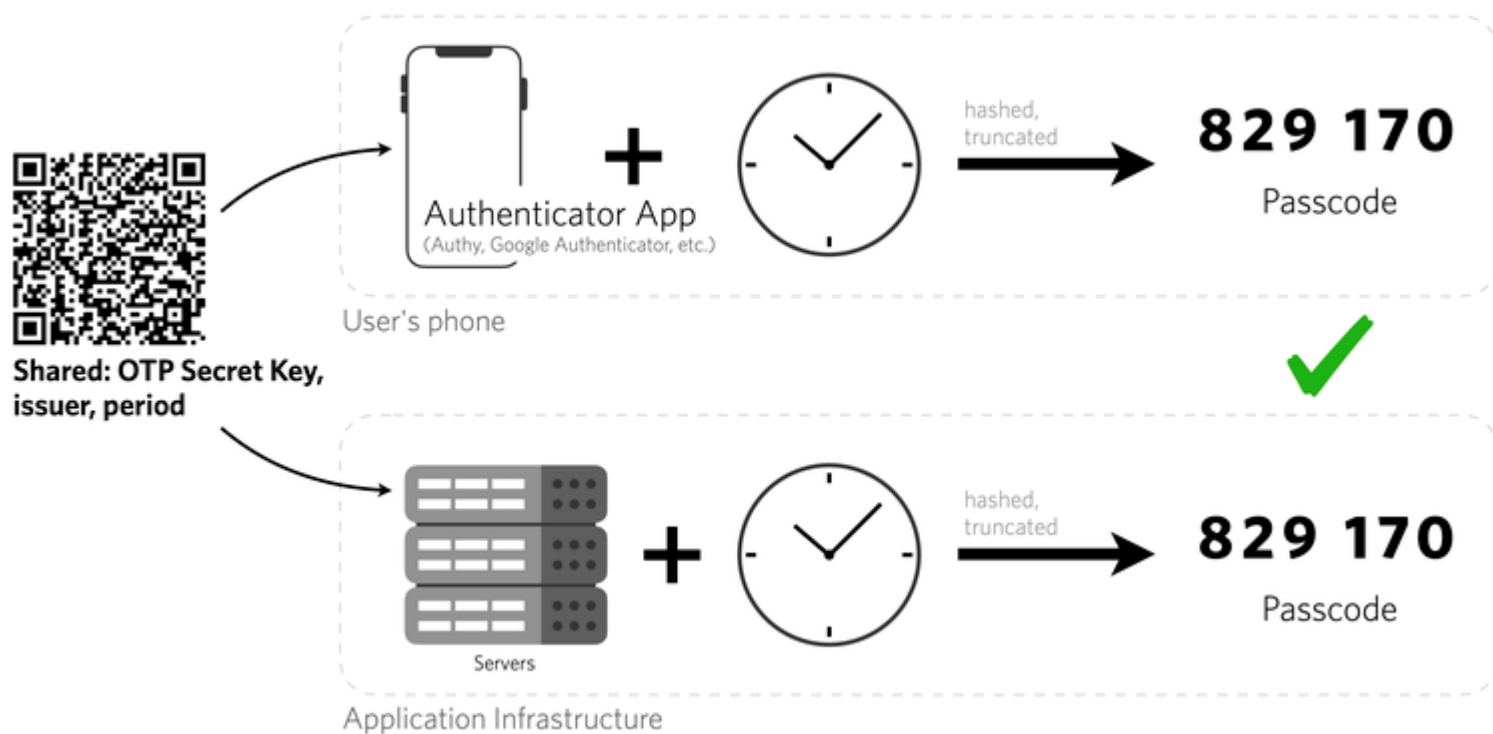
- Další vrstva ochrany k heslu

Typický druhý faktor:

- Software (aplikace běžící na chytrém telefonu)
 - jednorázové heslo
- Hardware:
 - token



TOTP



Google Authenticator

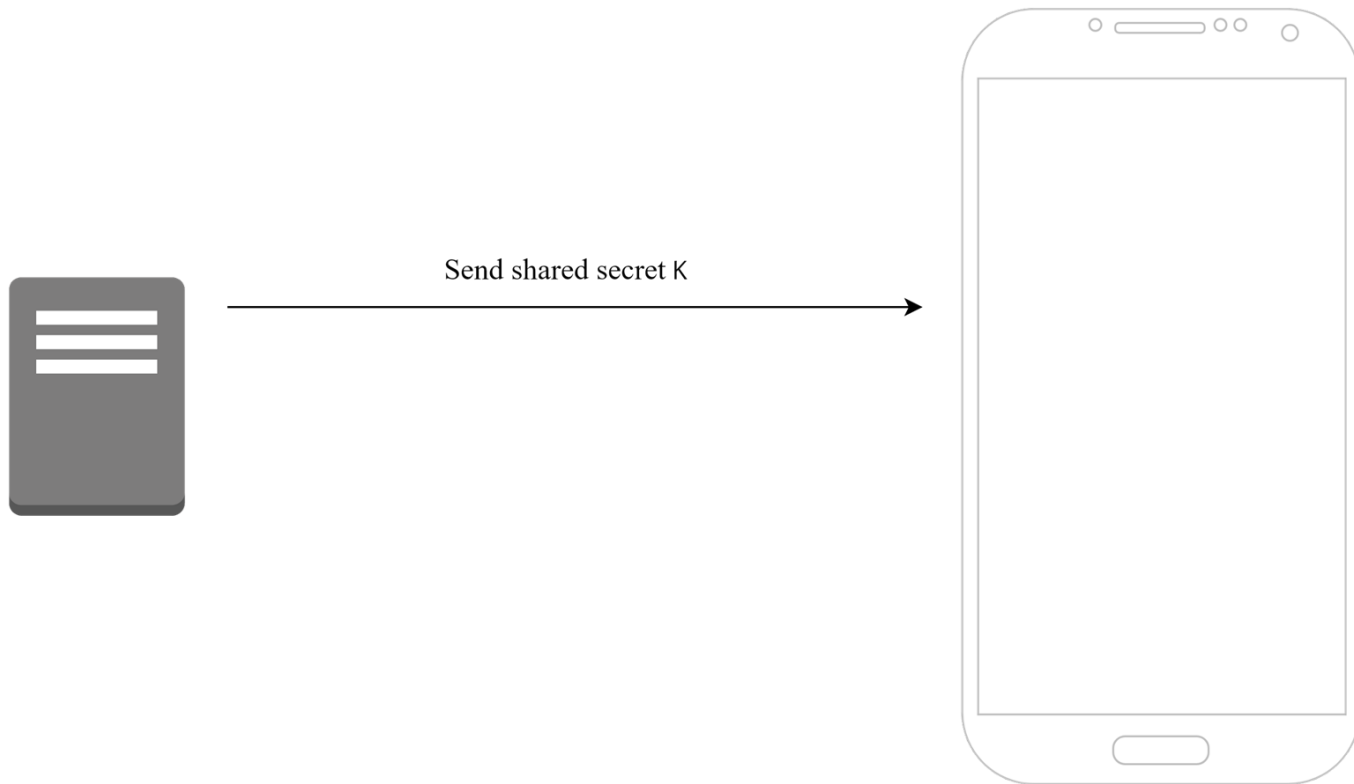
1. Tajný klíč **K** zná **služba** a uživatel (chytrý telefon)

Když se chceš autentizovat:

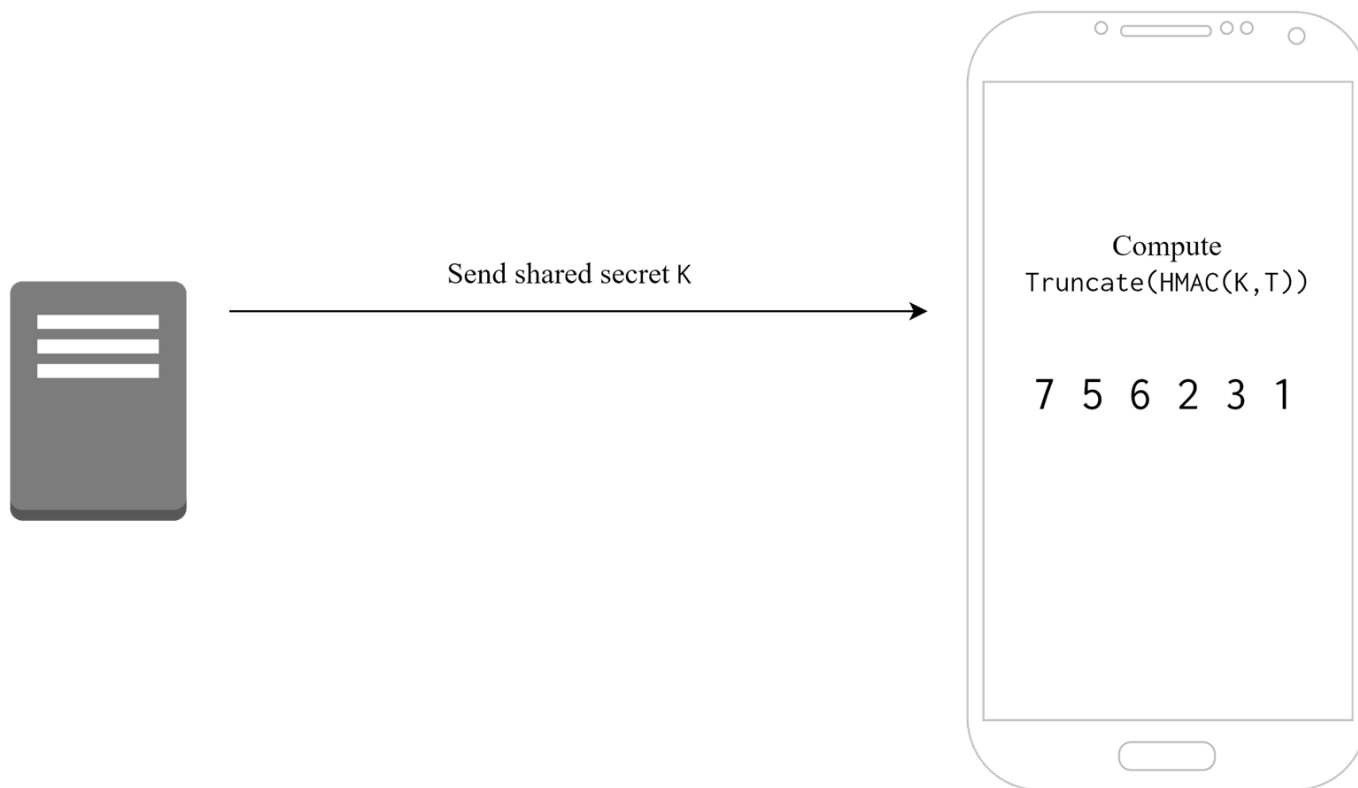
1. Výpočet $T = \text{aktuální čas} // 30 \text{ seconds}$
2. Výpočet $H = \text{HMAC}(K, T)$
3. Použij 6 posledních číslic jako jednorázové heslo

Služba zopakuje výpočet (1.-3.) a ověří tvé heslo/číslo.

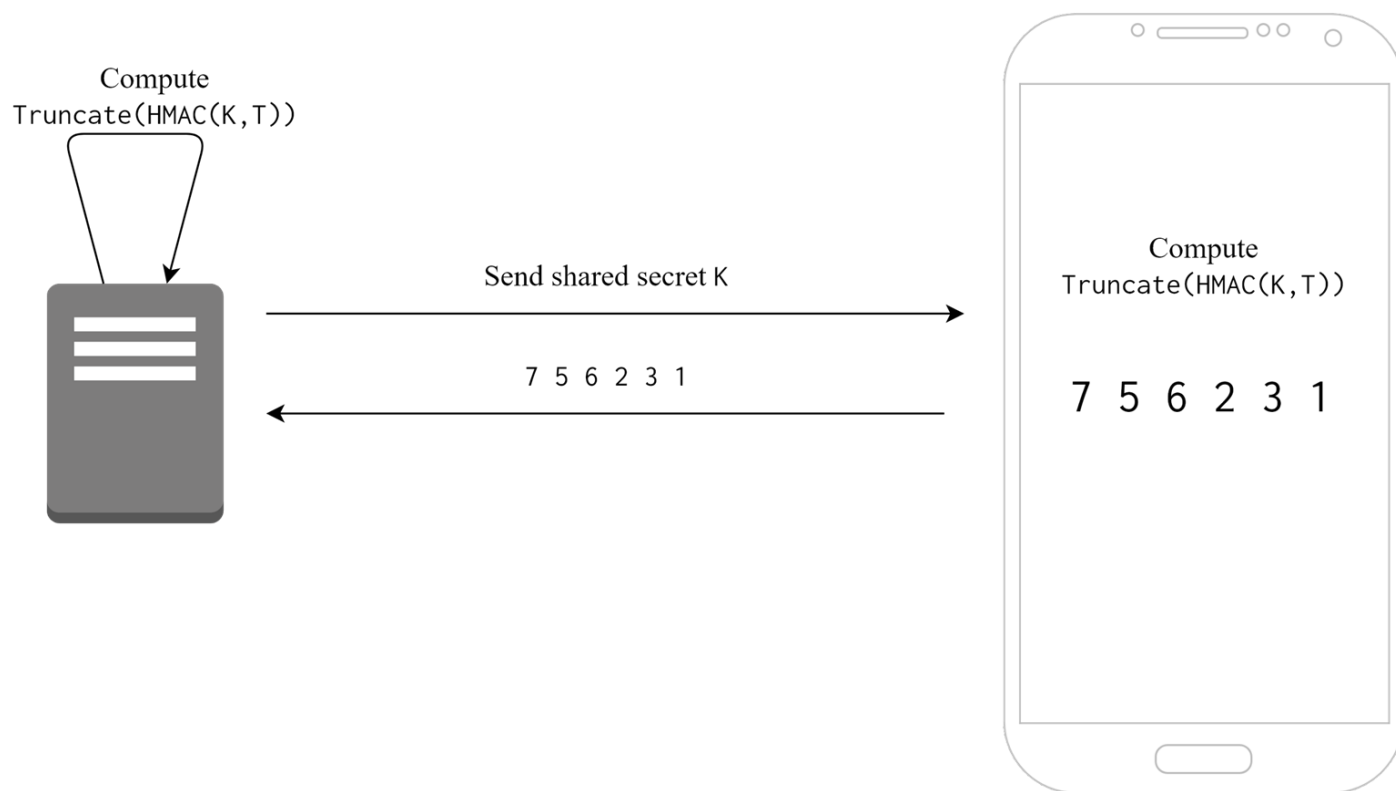
TOTP



TOTP



TOTP



Digitální podpis

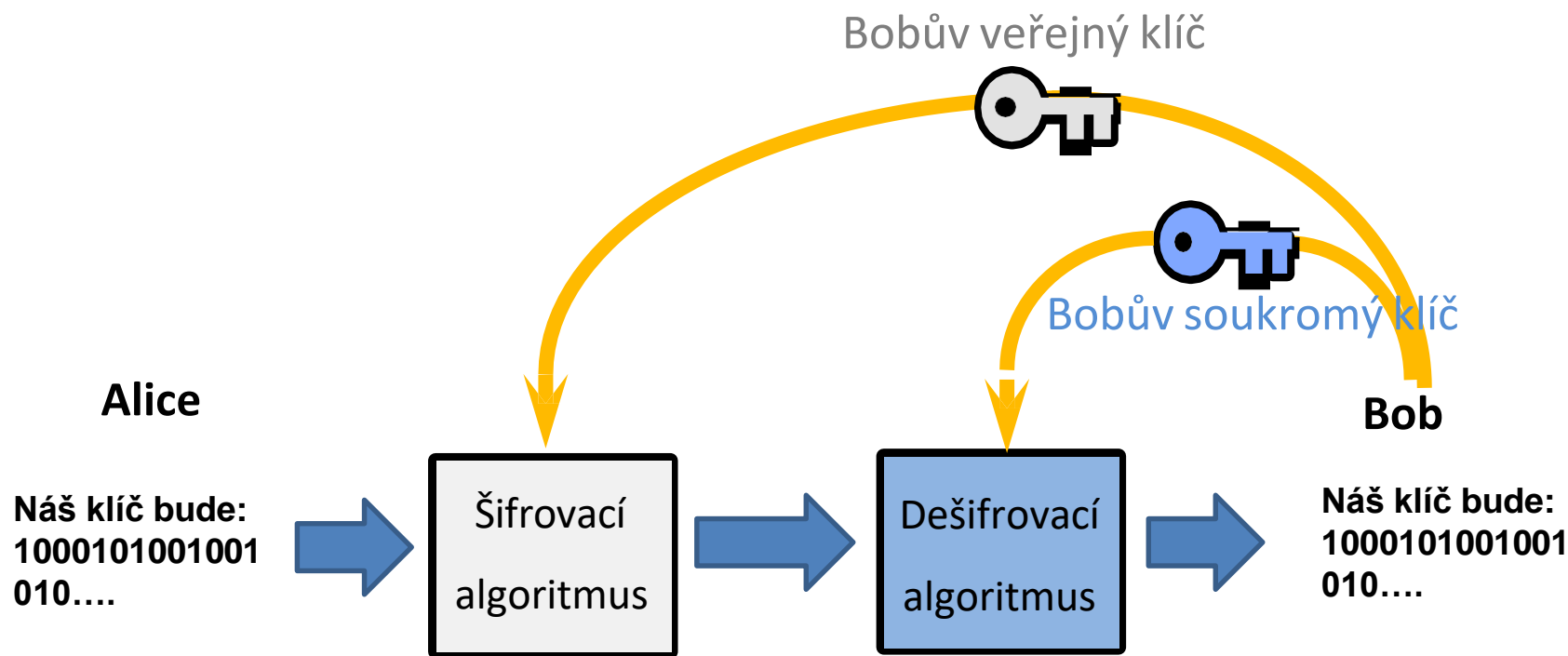
Klasické šifrování

- Klíč + správa \Rightarrow šifra \Rightarrow zašifrovaná správa
- Klíč je klíčový – kdo ho zná může šifrovat i dešifrovat (např. hesla zašifrovaná osobním heslem ve správci hesel)



<https://codebeautify.org/encrypt-decrypt>

Šifrování veřejným klíčem



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

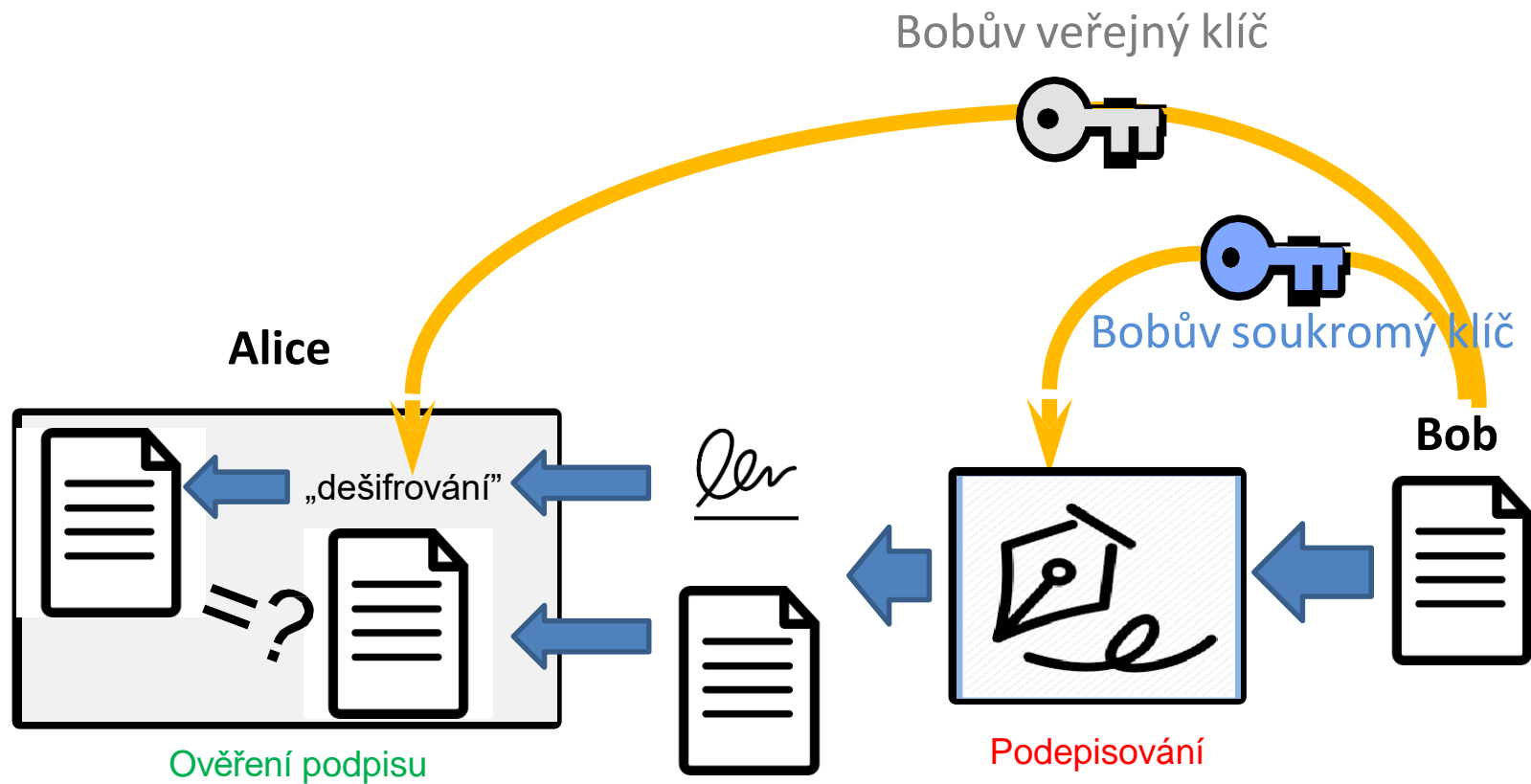
Bezpečné stránky

- šifrované spojení



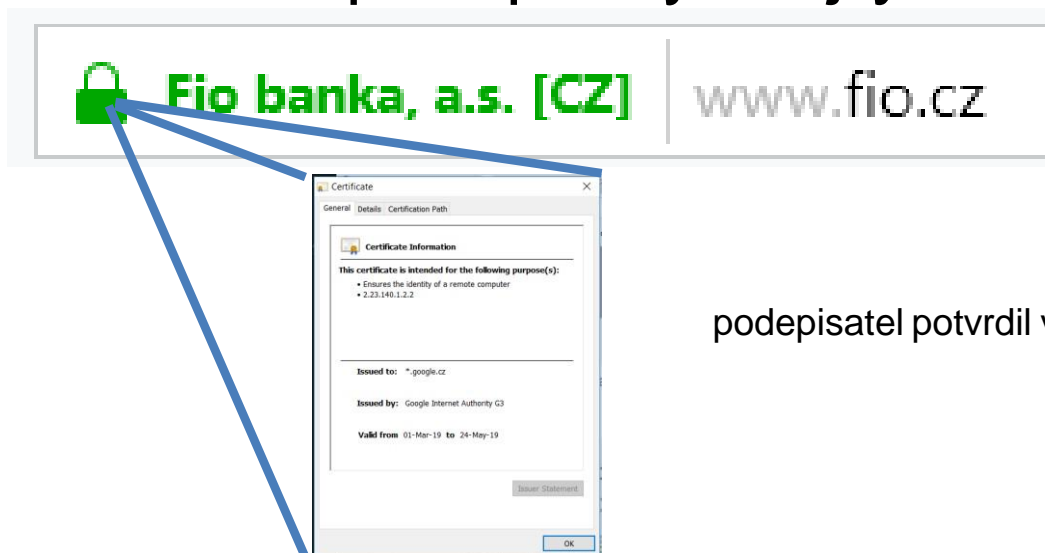
Digitální podpis

- podobý princip jako při šifrování veřejným klíčem



Certifikát

- Jak vím, že komunikuji 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