ŠIFROVÁNÍ DAT

ŠIFROVÁNÍ NEBOLI KRYPTOGRAFIE

- je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.

ŠIFRA, ŠIFROVÁNÍ

- kryptografický algoritmus, který převádí čitelnou zprávu/data na její nečitelnou podobu neboli *šifrový text/data*. *Klíč* je tajná informace, bez níž nelze šifrový text přečíst.

SYMETRICKÁ A ASYMETRICKÁ ŠIFRA

- *Symetrická šifra* je taková, která pro šifrování i dešifrování používá tentýž klíč.
- *Asymetrická šifra* používá *veřejný klíč* pro šifrování a *soukromý klíč* pro dešifrování.

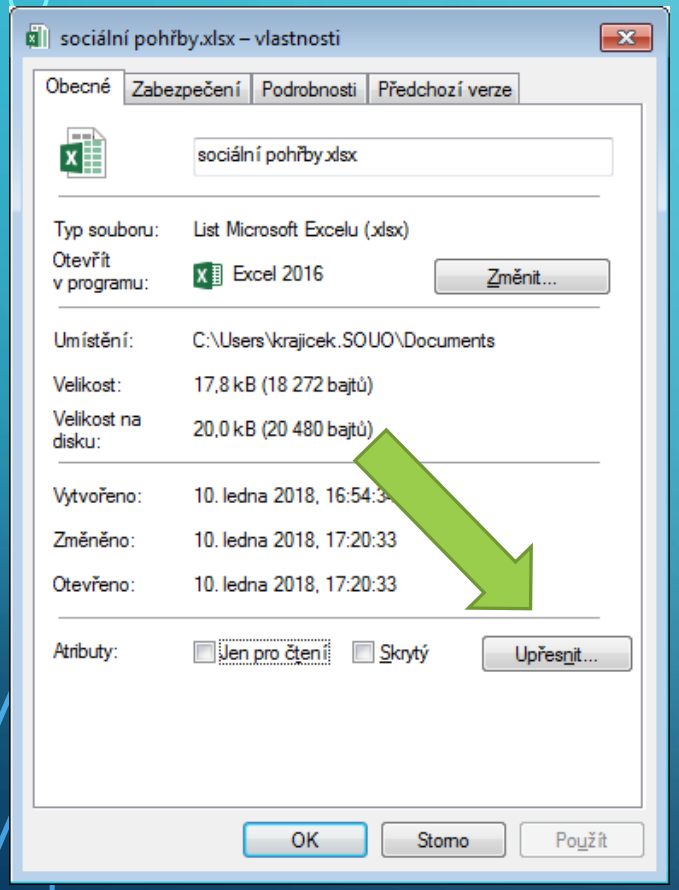
CERTIFIKÁT A ELEKTRONICKÝ PODPIS

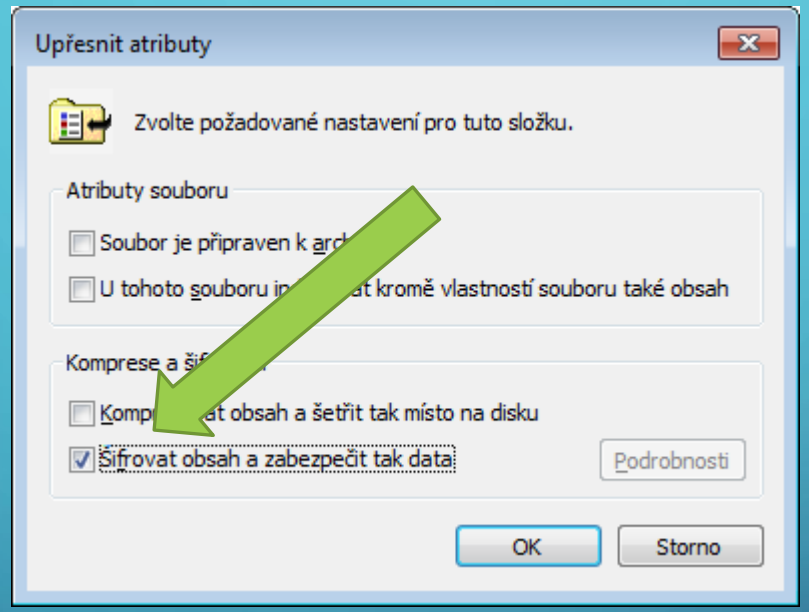
- jsou softwarové prostředky, které umožní šifrování dat

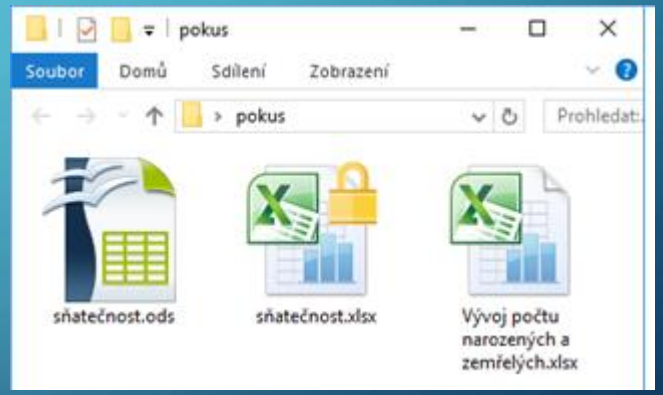
ŠIFROVÁNÍ SOUBORŮ

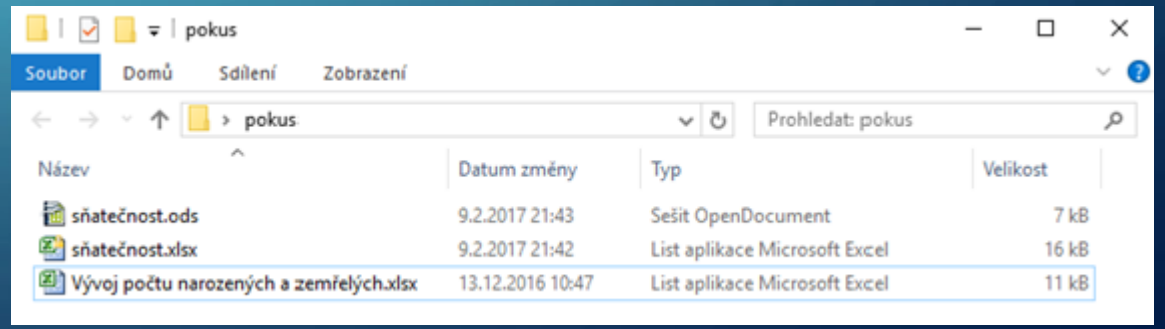
- je softwarové šifrování a dešifrování jednotlivých souborů, adresářů, částí pevných disků, výměnných médií, e-mailových zpráv
- Pokud se kódují velké objemy dat, bootování i práce se soubory se znatelně zpomalí
- lze použít i velmi rozšířené archivátory 7zip, WinRAR, …, nejlépe v samorozbalovacích archivech
- Šifrovat lze i novými OS (BitLocker Drive Encryption)

ŠIFROVÁNÍ SOUBORŮ VE WINDOWS 10









ŠIFROVÁNÍ EMAILŮ

- Šifrování emailů umožňuje zašifrovat zprávu pomocí veřejného klíče adresáta a zajistit, že nikdo kromě adresáta vlastnícího odpovídající soukromý klíč nebude moci email přečíst. Elektronický podpis umožňuje emailovému klientu příjemce pomocí veřejného klíče odesílatele ověřit, že přijatá zpráva je v přesně stejné podobě, v jaké byla odeslána. Zajišťuje tedy, že email skutečně odeslal majitel certifikátu a že na cestě k adresátovi případný útočník zprávu neodchytil a nepozměnil.
- Šifrování nabízí běžné plnohodnotné emailové klienty (Outlook, Apple Mail, Thunderbird)

ŠIFROVÁNÍ WI-FI

- **WPA2**, je dodatek k IEEE 802.11 standardu vylepšující autentizační a šifrovací algoritmus pro bezdrátové sítě Wi-Fi, nahrazuje WEP a WPA
- Šifrování pomocí WEP má mnoho bezpečnostních slabin, zastaralé, prolomené
- Šifrování WPA je předchůdcem WPA2

HTTPS

- Je nadstavba HTTP, zabezpečuje spojení mezi webovým prohlížečem a serverem před odposlouchávání a umožňuje ověřit identitu
- Používá asymetrické šifrování pomocí protokolu SSL nebo TLS obvykle na portu 443
- Ověření digitálním certifikátem, SMS
- Použití – e-shop, e-bankovnictví, vstup do vlastní sítě, osobní informace, …

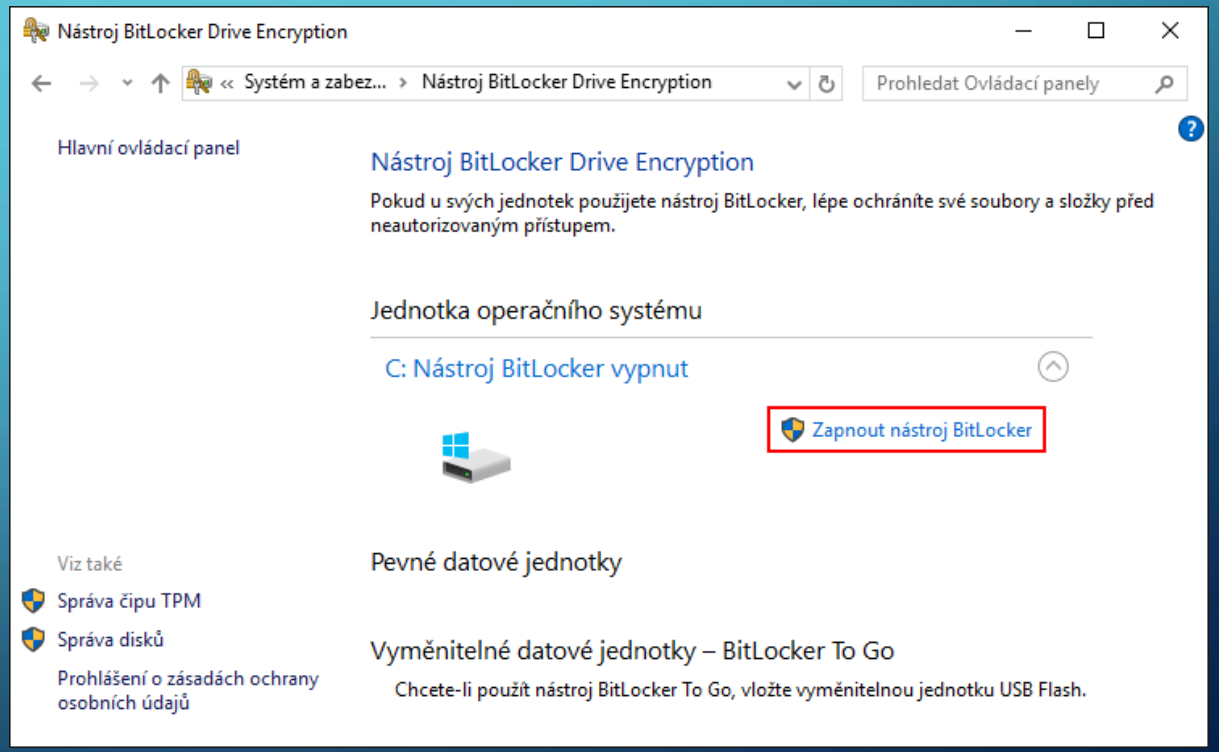
BitLocker

K odemknutí této jednotky zadejte heslo.

••••••••••••

Chcete-li při psaní zobrazovat heslo, stiskněte klávesu Insert.

Pokračujte stisknutím klávesy Enter.
Nástroj BitLocker obnovíte stisknutím klávesy Esc.



KONTROLNÍ OTÁZKY

- Jaký druh šifry byla scytale (skytale, skytála), jak a kdy se používala?
- Jaký je rozdíl v klíčích u symetrického a asymetrického šifrování?
- Co to je digitální podpis s certifikátem?
- Co znamená zkratka https://?
- Jaké kroky musíme provést pro zabezpečení domácí WI-FI sítě?
- Jak poznáme zašifrovaný soubor?
- Jak zašifrujete soubor v OS Windows 7 nebo 10