evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

PSK2-17

Název školy:	Vyšší odborná škola a Střední průmyslová škola, Božetěchova 3
Autor:	Ing. Marek Nožka
Anotace:	Úskalí šifrování veřejným klíčem
Vzdělávací oblast:	Informační a komunikační technologie
Předmět:	Počítačové sítě a komunikační technika (PSK)
Tematická oblast:	Vrstvy protokolu TCP/IP
Výsledky vzdělávání:	Žák popíše funkci a důvody vzniku certifikačních autorit a pavučiny důvěry
Klíčová slova:	asymetrická šifra, Alice, Bob, certifikační autorita, web of trust
Druh učebního materiálu:	Online vzdělávací materiál
Typ vzdělávání:	Střední vzdělávání, 3. ročník, technické lyceum
Ověřeno:	VOŠ a SPŠE Olomouc; Třída: 3L
Zdroj:	Vlastní poznámky, Wikipedia, Wikimedia Commons

Šifrování a elektronický podpis II

Hybridní systémy

Symetrické šifry se často používají společně s asymetrickými. Využije se tak výhod obou dvou systémů: odpadá problém distribuce klíčů a zároveň je systém dostatečně rychlý.

Obvyklé použití je takové, že otevřený text se zašifruje symetrickou šifrou s náhodně vygenerovaným klíčem. Pro každou zprávu (session) se generuje jiný (nový) klíč. Tento symetrický klíč se zašifruje veřejným klíčem asymetrické šifry, takže dešifrovat data může pouze majitel tajného klíče dané asymetrické šifry.

Asymetrická šifra takto slouží jako bezpečný kanál pro přenos symetrického klíče.

Hašovací funkce, Hash, Otisk, Fingerprint

Hašovací funkce je matematická funkce (algoritmus) pro převod vstupních dat do (relativně) malého čísla. Výstup hašovací funkce se označuje výtah, miniatura, otisk, fingerprint či hash (česky též někdy jako haš).

Nejznámější hashovací funkce jsou MD5, CRC nebo SHA.

Hašovací algoritmy jsou bezpečné pokud je velmi obtížné (tj. se současnými prostředky prakticky nemožné):

1. najít zprávu, která odpovídá svému otisku
2. najít dvě rozdílné zprávy, které mají stejný otisk

Například následující zpráva:...

```
Alenko!

Oběd máš v lednici. Vrátím se až večer.

    Máma
```

`--> stáhnout

... má tento MD5 otisk:

```
b99ed1417ff6469b94a605b9c789c161
```

a tento SHA1 otisk:

```
834bfc7d8ced0c10963dd8ef9123020bd441f450
```

Pokud změním zprávu, změní se i otisky. Všimněte si, že různě dlouhé zprávy mají vždy stejně dlouhé otisky.

```
Alenko!

Oběd máš v lednici. Vrátím se až večer.

--
Ahoj
   Tvoje Máma
```

`--> stáhnout

MD5:

```
b35d7d1cc5874b6440f1eb0cca312314
```

SHA1:

```
7badc8f34d34ef422b833071dc7529595d958e19
```

Jestliže mají dvě zprávy stejný hash je velká pravděpodobnost, že se shodují. Hašovací funkce se mimo jiné používá u elektronického podpisu a při ověření pravosti klíčů. **Pokud mají dva klíče stejný hash je vysoce pravděpodobné, že i klíče jsou stejné.**

Problém výměny klíčů

Mohlo by se zdát, že se zavedením veřejného klíče zmizel problém distribuce klíčů -- klíč je přece (už v principu) veřejný a tak ho lze bez obav šířit. Celý systém má ale následující slabinu: **Každý, kdo systém používá si musí být jistý identitou veřejných klíčů.** Jinak řečeno: musím si být jistý, že klíč na kterém je jmenovka Alice, opravdu patří Alici. Musím si být jistý, že klíč o kterém se prohlašuje, že patří Bobovi skutečně Bobovi patří. Pokud bychom tuto jistotu neměli mohla by do komunikace vstoupit třetí osoba a komunikaci odposlouchávat. Tento problém se označuje jako Man in the middle.

Nabízí se samozřejmě myšlenka předávat si klíče osobně "z ruky do ruky", ale zde bychom se vrátily k problémům, které měla konvenční symetrická šifra.

V praxi se používá ověření identity klíče pomocí jeho hashe -- fingerprintu. Pokud obdržím od svého korespondenta jeho veřejný klíč, nejprve například po telefonu ověřím svůj a jeho fingerprint, abych zjistil, že mám pravý klíč.

I to ověření může být často obtížné a proto se používá Síť důvěry (Web of trust) nebo Certifikační autorita.

Software

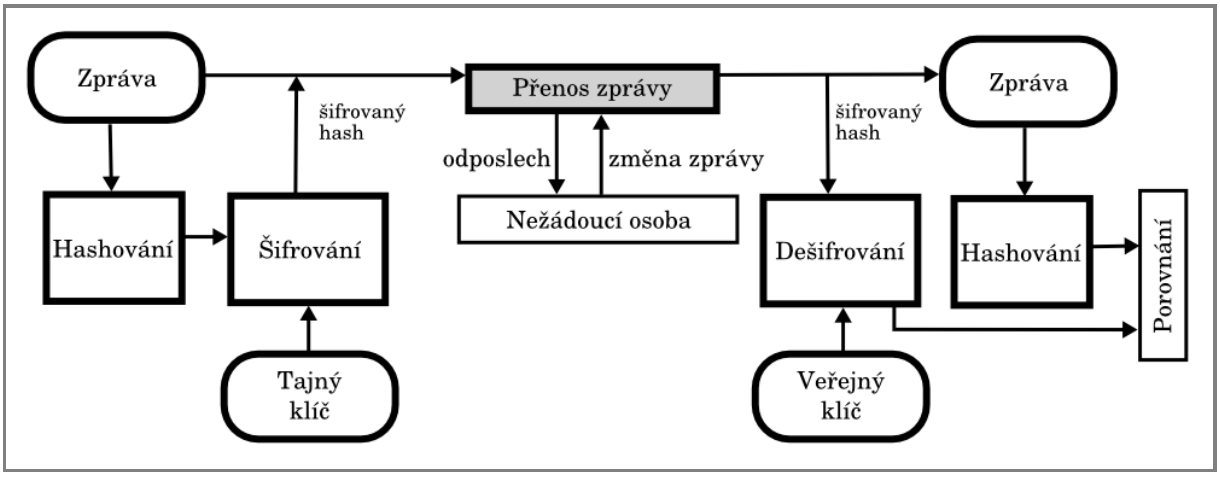
Prvním software vůbec, který implementoval asymetrickou šifru byl PGP -- Pretty Good Privacy, jehož autorem je Phil Zimmermann a který mimo jiné stal předmětem soudního sporu, protože byl považován za zbraň.

Další známou implementací, která splňuje OpenPGP standard je GPG -- GNU Privacy Guard.

Oba výše zmíněné programy využívají principu web of trust. Většina ostatních programů, umožňující zabezpečenou komunikaci, jako jsou webové prohlížeče a e-mailový klienti oproti tomu používá systém certifikačních autorit a knihovnu SSL respektive TLS.

Jak funguje elektronický podpis?

1. Ze zprávy se vytvoří Hash
2. Hash se zašifruje pomocí privátního klíče a připojí se ke zprávě
3. Na přijímací straně se hash pomocí veřejného klíče rozšifruje.
4. Na přijímací straně se znovu ze zprávy vytvoří hash.
5. Přijatý a přenesený hash se porovnají.



Algoritmy

- RSA
- ElGamal
- Diffieho-Hellmanova výměna klíčů
- DSA -- Digital Signature Algorithm