PGP

* PGP=Pretty Good Privacy, ”šifrování s veřejným klíčem pro masy”
* Phil Zimmermann, zač. 1984, uvolněn 1991

* problémy s patentem na RSA (1994)
 - proto legální verze 2.6 vytvořená na MIT úmyslně generuje zprávy, podpisy a klíče které verze starší než 2.3a neumějí přečíst
 - nové verze PGP umějí přečíst všechny formáty
* nakonec další verze komerčně (ViaCrypt, Network Associates)
* od roku 1999 se může z US legálně vyvážet
 - nejnovější verze PGP 8.0 (PGP Corporation)

* velká část SW věnována správě klíčů
* základní protokol využívá RSA, IDEA a MD5 (specifikován v RFC1991)
* později specifikace OpenPGP (RFC2440) - nový formát řeší potíže předchozího, přidává asymetrické algoritmy ElGamal (odvozený z DH) a DSS (Digital Signature Standard) a symetrické 3DES (EDE, jako nejmenší společný jmenovatel různých implementací), dále CAST5 (viz RFC2144), SAFER-SK128 a hashovací fce SHA-1 (povinné), RIPEMD160 a MD2; MD5 je pouze doporučené
* nejnovější verze implementují i AES

* pro generování dvojice veřejný/tajný klíč použity náhodné bity získané měřením doby mezi stiskem kláves
 - verze pod Windows - pohyb myší
 - pod UNIXem lze spouštět různé programy a vytvářet hash jejich výstupu (vmstat, netstat -s, uptime, ipcs -a apod.)
 - pod Linuxem můžeme číst /dev/random
* pro každou zprávu konvenční relační klíč generován pomocí IDEA ze seed a dalších náhodných bitů
 - klíč zašifrován veřejným klíčem příjemce, zašifrovaný relační klíč zaslán spolu se zprávou
 - zpráva šifrována relačním klíčem pomocí IDEA v 64bitovém CFB módu
 - data zprávy před šifrováním komprimována (to snižuje redundanci a tím zvyšuje bezpečnost, používá algoritmy z PKZIP - RFC1950), krátké a špatně komprimovatelné zprávy nekomprimuje
 - pokud je zpráva podepsána, je zašifrována včetně podpisu

* digitální podpis: 128bitový digest zprávy pomocí MD5 + časové razítko zašifruje tajným klíčem odesilatele

* GnuPG (GNU Privacy Guard) jako alternativa od FSF
 - příklad použití gpg:

```
$ gpg --gen-key                 # generování dvojice tajný/veřejný klíč
$ gpg --list-keys               # vypíše seznam klíčů
$ gpg -a --export [Alice]       # export všech nebo určených klíčů na stdout
$ gpg --import soubor           # import klíčů ze souboru

$ gpg --clearsign soubor.txt    # podepíše soubor + přidá příponu .asc
$ gpg --verify soubor.txt.asc   # ověří podpis

$ gpg -a -r Bob -e soubor.txt   # zašifruje + vytvoří .asc soubor
                                # pokud se nepoužije -a, vytvoří binární .gpg
$ gpg soubor.txt.gpg            # dešifruje soubor
```

* certifikáty, síť důvěry (”web of trust”)
 - při přijetí veřejného klíče v PGP specifikuji, zda je klíč důvěryhodný pro certifikaci dalších klíčů (volby: unknown, untrusted, marginally trusted, completely trusted)
 - klíč podepsaný některým důvěryhodným (”completely trusted”) klíčem je považován za platný
 - pro jiné typy důvěry vážený součet, např. za platný považován klíč může být považován klíč podepsaný dvěma částečně důvěryhodnými (”marginally trusted”) klíči; možno nastavit, klíč důvěryhodný pokud součet >= 1
 - tj. uživatelé mohou uvádět další uživatele, decentralizovaný přístup

* na síti servery poskytující klíče přes rozhraní WWW, ftp, e-mail

* nejslabším článkem - není možné zaručit, že nikdo nepoužije kompromitovaný klíč; pokud zjistíme, že klíč je kompromitován, vydáme tzv. certifikát odvolání klíče (key revocation certificate), ale nemůžeme zaručit, že ho uvidí všichni potenciální odesilatelé

* podpora PGP případně GnuGP je zabudována do většiny volně šířených e-mailových klientů, používá se zejména pro digitální podpisy
* další aplikace PGPfone (Pretty Good Privacy Phone)

Další způsob šifrování e-mailů PEM (Privacy Enhanced Mail 1993 - viz RFC1421 až RFC1424) se příliš neuchytil, protože vyžaduje striktní hierarchii certifikačních autorit, nezašifrovaná hlavička zprávy poskytuje informaci o odesilateli a příjemci.

* nelze spoléhat pouze na kryptografii
 - skutečný oponent udělá všechno pro to, aby věci fungovaly nejhorším možným způsobem v nejhorší době
 - útok většinou něco, co návrhář systému nepředpokládal => obtížné se bránit
 - tj. otázka není ZDA nastane problém, ale KDY nastane
 - je zapotřebí mít připravenou cestu jak obnovit bezpečnost

Získali jsme základy z šifrování, můžeme se podívat na nekryptografické metody ochrany.

Autentizace uživatelů

* uživatel se chce autentizovat = prokázat svou identitu systému
* většina metod založená na identifikaci
  1. něčeho co uživatel zná (autentizace pomocí hesel apod.)
  2. něčeho co uživatel má (má autentizační předmět)
  3. něčeho co uživatel je (biometrické metody)

Autentizace pomocí hesel

* nejčastější forma - uživatel zadá jméno a heslo
 - ověření dvojice jméno a heslo - viz předchozí dvě přednášky (Kerberos, autentizace v UNIXových systémech)
 - při zadávání hesla by se nemělo heslo zobrazovat, aby ho Oskar nemohl zahlédnout
 - například:
  . UNIX při zadávání hesla nezobrazuje nic
  . Windows 2000 zobrazuje hvězdičku pro každý znak => Oskar může zjistit délku
 - reakce na chybu by neměla Oskarovi poskytnout užitečné informace, např.
  . správné přihlášení (a) a dva způsoby reakce na chybu (b) a (c)

```
 a) LOGIN: luki        b) LOGIN: lukas         c) LOGIN: lukas
    PASSWORD: foobar      INVALID LOGIN NAME      PASSWORD: nope
    SUCCESSFUL LOGIN      LOGIN:                  INVALID LOGIN
```

  . v případě (b) systém ohlásí chybu jakmile je zadáno chybné uživatelské jméno; považuje se za chybu, protože Oskar může zkoušet přihlašovací jména dokud nenajde správné
  . v případě (c) se systém vždy zeptá na heslo a neposkytuje informaci zda je přihlašovací jméno samo o sobě platné

Autentizace typu výzva-odpověď

* alternativa k systému hesel - mít dlouhý seznam otázek a odpovědí uložených bezpečně na serveru
 - otázky zvoleny tak, aby si uživatel odpovědi nemusel zaznamenávat, např.
  1. Jak se jmenovala maminka za svobodna?
  2. Jak se jmenuje Petry nejstarší sestra?
  3. V jaké ulici se nacházela tvoje základní škola?

```
  4. Jak se jmenoval tvůj třídní učitel v první třídě?
 - při přihlášení systém náhodně vybere otázku a zkontroluje odpověď
 - je praktické pouze při velkém množství párů otázek a odpovědí

* jiná variace - uživatel si vybere algoritmus, např. x^2
 - při přihlašování systém zobrazí argument, např. 7
 - uživatel odpoví 49
 - algoritmus se může lišit ráno a večer, různé dny v týdnu apod.

* pokud má terminál výpočetní výkon (např. uživatel se přihlašuje z mobilního
  telefonu), můžeme využít kryptografický protokol typu výzva-odpověď
 - uživatel a server sdílejí symetrický klíč K
 - server pošle výzvu r_B
 - terminál vypočte odpověď K(B, r_B)


Autentizace pomocí autentizačního předmětu
------------------------------------------

* základní myšlenka - ověření identity pomocí fyzického objektu, podobně jako
  máme klíč od domu
* dnes většinou karta (např. kreditní karta, JIS, karta do SVK atd.)

* kartu vložíme nebo přiložíme ke čtecímu zařízení; aby někdo nemohl zneužít
  zapomenutou kartu, vyžaduje se často ještě zadání hesla (např. PIN)

* nejjednodušší mechanismus - karty s magnetickým proužkem, například kreditní
  karty
 - na zadní straně karty magnetický proužek obsahující cca 140 bytů informace
 - na kartě PIN zašifrované pomocí tajného klíče banky
 - výhoda: levné, jedna karta stojí cca 3 Kč
 - nevýhoda: zařízení pro čtení a zápis karet jsou běžně dostupná, není
   problém kartu duplikovat => není příliš bezpečné (banky mají dobré
   právníky, takže jim to nevadí)

* čipové karty - mohou být dále rozděleny na karty s pamětí a inteligentní
  karty
 - karty s pamětí (stored value cards)
  . obsahují malé množství paměti (E)PROM (obvykle < 1 KB)
  . čtecí/zapisovací zařízení čte a zapisuje paměť
  . dříve jako telefonní karty; jako autentizační předmět se nepoužívají
 - inteligentní karty (smartcards) - mnohem univerzálnější použití
  . technicky např. 8 bitový CPU na 4 MHz, 16 KB ROM, 4 KB EEPROM, 512 bytů RAM,
    sériový komunikační kanál 9600 bps, někdy kryptografický koprocesor,
    případně JVM v ROM
  . s časem se zlepšuje, ale omezeno velikostí čipu a cenou (150-1500 Kč)
  . mnoho různých použití (například ukládání zdravotních informací apod.),
    ale nás v BIT zajímají pouze souvislosti s bezpečností
  . inteligentní karty jako autentizační předměty: protokol typu výzva-odpověď, klíč
    uložen na kartě
  . nevýhoda - pokud je karta ukradena, může jí Oskar libovolně analyzovat
    (pokoušet se najít klíč pomocí timing & power consumption attacks,
    vyzařování, vkládání chyb apod.)


Autentizace s využitím biometrických informací
----------------------------------------------

* typický biometrický systém má dvě části
 - zápis uživatele (enrollment) - snímací zařízení změří a digitalizuje
   vlastnosti uživatele, systém uloží identitu uživatele a vlastnosti
   podstatné pro identifikaci
  . záznam buď v centrální databázi nebo na smardcard
 - identifikace - uživatel zadá své jméno, systém provede měření a porovná s
   hodnotami uchovanými během zápisu
  . úloha ověřit zda charakteristika odpovídá zadanému uživateli rychlejší i
    bezpečnější než najít uživatele podle charakteristiky - proto se zadává
    jméno; některé systémy umí obojí
 - výhoda - na rozdíl od jiných mechanismů vyžaduje fyzickou přítomnost
```

osoby; zatímco mou kartu si Oskar může opatřit, mojí sítnici si opatřit nemůže

* jaké charakteristiky lze použít?
 - musí mít dostatečnou variabilitu aby bylo možné lidi rozpoznat (proto nelze použít např. barvu vlasů)
 - musí být psychologicky akceptovatelné (např. snímání otisků prstů nemusí být v některých zemích pro uživatele přijatelné)
 - informace by měl být prakticky získatelná (tvar ucha vs. vlasy dívek)
 - nemělo by se příliš měnit s časem (např. rozpoznávání obličeje pokud si uživatel nechá narůst vousy nebo uživatelka se namaluje)
  . nejvýhodnější pokud se databáze upravuje při každém použití
 - odolnost proti podvodům
 - první systémy nebyly komerčně úspěšné, protože pomalé (2-3 osoby za minutu je málo)

* tradiční metody:
 - otisky prstů
 - charakteristiky očí - sítnice a duhovka
 - rozpoznávání obličeje
 - geometrie ruky
 - rozpoznávání hlasu

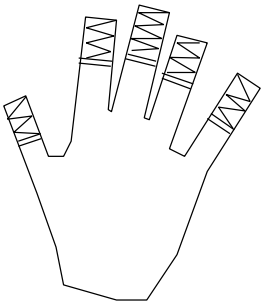
* otisky prstů
 - způsoby snímání: elektrické, termální, optické a hybridní (elektro-optické); problémy se špínou na snímačích => nové snímače ultrazvuk
 - výhoda: otisky prstů jedinečné
 - nevýhody: pokud uživatel denně píše na počítači, hraje na klavír apod. mohou být papilární linie tenké => obtížné sejmout
  . podobně při genetických defektech nebo zraněních
  . v zimě může být praktický problém nutnost sundat rukavice
 - snímače komerčně dostupné, používají některé firmy; některé snímače kombinované se čtečkou inteligentní karty (Veridicom)
 - výrobci automobilů - výzkum pro účely odemykání auta, řízení apod.

* sítnice - snímač (retina scanner) snímá vzor žilek v sítnici, také jedinečný
 - sítnici osvětlí zdroj světla nízké intenzity, optické zesílení (původně se používal červený laser, problém s akceptovatelností)
 - vyžaduje podívat se do snímače a zaměřit na určený bod
 - ověření zda není statický obraz - zkontrolování pulsu viditelného na sítnici
 - potíže
  . uživatelé s kontaktními čočkami, uživatelé pro které je nepříjemný blízký kontakt se čtecím zařízením, nevidomí a lidé se zraněním sítnice
  . může poskytnout informaci o zdravotním stavu (neidentifikuje => nějaký zdravotní problém způsobil změnu na sítnici)
 - používá se kde je zapotřebí vysoká míra bezpečnosti, např. ve vojenských instalacích

* duhovka - nevyžaduje blízký kontakt, postačuje kamera
 - rozpoznává se vzor vláken v duhovce
 - nemá potíže s brýlemi a kontaktními čočkami (pokud je dobré osvětlení)
 - problémy: nevidomí, vzor se může změnit z důvodu nemoci nebo zranění
 - používají některé letecké společnosti pro urychlení odbavení stálých zákazníků

* rozpoznávání obličeje - snímání běžnou kamerou
 - zatím lze zmást pokud se vzhled změní (vousy, brýle, makeup, stárnutí, neobvyklý výraz obličeje
 - jednoduché systémy můžeme zmást podstatnou změnou orientace obličeje vůči kameře (15 stupňů zhorší schopnost rozpoznat, ve 45 stupňů už nerozpozná)
 - varianta - infračervené snímání, rozložení krevního řečiště v obličeji
  . spolehlivější rozpoznání, předpoklad práce v noci
 - používá se spíše pro rozpoznání nezvaných návštěvníků, např. některá kasina pro rozpoznání podvodníků

* rozpoznávání geometrie ruky
 - měření délek prstů - technicky jednoduché a praktické



- nevýhoda - je možné vytvořit duplikát z umělé hmoty apod.

- lepší systémy - měří také šířku a kontury prstů
- nevýhoda - ruce nesmí být oteklé, problém s genetickými defekty

❇