O čem bude tento předmět

* vlády, firmy i jednotlivci vlastní hodnotné informace, které potřebují ochranu, např.
  - vojenství: plány, rozmístění jednotek, družicové snímky apod.
  - firmy: informace o konkurenci, obchodní plány apod.
  - technické informace: software, design integrovaných obvodů apod.
  - osobní informace: dopisy, adresáře, zdravotní dokumentace apod.

* dokud byly tyto informace uchovávány v kartotékách, stačila fyzická ochrana: sejfy, zámky, alarmy, ...
* to ale nepostačuje pro data uchovávaná v počítačích:
  - ochrana informací uvnitř systému - aby nemohly přistoupit neautorizované programy
  - ochrana před neautorizovaným přístupem prostřednictvím počítačových sítí
  - ochrana před přístupem k informacím přenášeným počítačovými sítěmi

Z bezpečnostního hlediska řešíme následující problémy:

* důvěrnost dat = tajná data mají zůstat tajná
  - přesněji řečeno, data mají být přístupná pouze autorizovaným uživatelům (tj. těm, o kom vlastník dat rozhodl, že jim mají být přístupná)

* integrita dat = neautorizovaní uživatelé nesmějí moci modifikovat data (např. rušit existující data, přidávat vlastní)

* autentizace = ověření s kým mluvíme

* neodmítnutelnost (nonrepudiation)
  - jak můžeme dokázat zákazníkovi, že si od nás něco objednal?
  - týká se elektronických podpisů

* dostupnost systému = nikdo nesmí být schopen způsobit nepoužitelnost systému (útoky typu ”denials of service” (DoS))
  - v rámci OS - způsobím zátěž, zaberu paměť
  - po síti - pošlu záplavu požadavků
  - zatímco s důvěrností a integritou dat si dokážeme celkem dobře poradit, s útoky typu DoS se zachází hůře

Dalším aspektem - méně technickým a více politickým - je soukromí = ochrana jednotlivců před zneužitím informací o nich.

Kdo má zájem nám škodit?

* v literatuře o bezpečnosti název intruder (vetřelec), adversary (protivník), ve vojenské literatuře enemy (nepřítel)
  - v češtině budeme používat název ”oponent”

Ve chvíli, kdy zabezpečujeme systém, potřebujeme vědět, proti komu ho chráníme, jakou může mít motivaci, znalosti a vybavení.

1. Netechničtí uživatelé
   - běžní uživatelé - pro jejich odstavení stačí základní technické bariéry - přístupová práva apod.
   - ”script kiddies” - nemají znalosti, ale používají existující nástroje vytvořené zkušenými programátory přístupné na síti a na ”divokých” bulletin boardech
2. Techničtí uživatelé (studenti, systémoví programátoři apod.)
   - přijde jim zajímavé vyzkoušet si síly proniknutím do systému apod.
   - jsou autory nástrojů používaných (2)
3. Pokusy jednotlivců o zisk
   - např. bankovní programátoři - např. zaokrouhlené částky na jejich účet, vyčerpání dlouho nepoužívaných účtů až po vydírání (”Zaplaťte mi nebo...”)

  - ukradení záznamů a jejich prodej konkurenci apod.
4. Komerční a vojenská špionáž
  - pokus získat technologii, obchodní nebo vojenské plány apod.
  - na rozdíl od předchozích bývá finančně dobře podpořeno => oponent
    může mít k dispozici neobvyklou technologii apod.

* ochránit systém před vojenskou špionáží je zcela něco jiného, než
  zabránit studentům aby na školním stroji spustili IRC server
 - k dispozici např. technologie pro odposlech elektromagnetického
   vyzařování

Poznámka:

  Ke ztrátě cenných dat může dojít také náhodou (HW a SW chybami,
  lidskou chybou apod.) - ve skutečnosti k tomu
  dochází častěji než v důsledku promyšlených útoků oponentů.

  Řešení zálohovat - zálohy nejlépe daleko od původních dat.

[]

Od vynálezu písma lidé řešili problém jak dopravit zprávu tak, aby se
její obsah nedozvěděl oponent. Z dnešního hlediska dělíme metody do 2
kategorií:

* steganografie (z řec. steganos = zakryté, tajné)
 - doslova ”utajené psaní” - utajíme existenci zprávy
* kryptografie (z řec. kryptos = skrytý)
 - kódujeme tak, aby oponent o obsahu zprávy nic nezjistil

Historická steganografie
========================

* jedna z prvních zmínek je v Héródotově ”Historii”
 - Demeratus potřeboval oznámit Spartě, že Xerxes chce napadnout Řecko
 - seškrábal vosk z tabulek, zprávu napsal na dřevo, pokryl
 - tabulky vypadaly jako nepoužité - prošly strážemi

* modernější forma - neviditelné inkousty
 - známé jsou mléko, ocet, moč
 - výše zmíněné tmavnou při zahřátí

* historicky detekce - viz heslo Dechiffrování v Riegerově ”Slovníku
  naučném” II/2, Praha 1862:

  Chceš-li se přesvědčiti, zdali na bílém papíře, o kterém se domýšlíš
  že neviditelné písmo na sobě nese, skutečně něco psáno jest, udělej
  následující zkoušky v tomtéž pořádku, jak zde uvedeny jsou, po sobě:

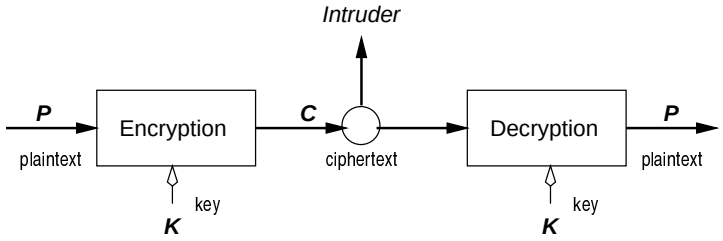
  1. Drž papír proti světlu, zdali snad písmo prosvítá (stane se to,
     je-li papír bílým inkoustem popsán)
  2. Polož papír na arch ssavého papíru napojeného louhem ze dvou částí
     živého vápna a jedné části kamenky (auripigment) svařených ve
     vodě, a ponech ho tam asi půl hodiny.
  3. Drž papír nad žhavým uhlím.
  4. Polož ho na půl hodiny do čisté vody.
  5. Usuš papír a posyp jej po obou stranách práškem z uhlí neb sazí,
     pak tento pomalu odfoukni.
  6. Potři papír po obou stranách tence černidlem; písmo vyvstane a
     ukáže se černější.

  Neobjeví-li se písmo po žádné z těchto zkoušek, pak není zajisté nic
  tam psáno.

* s technologií pro detekci - lepší inkousty, které reagují pouze na
  určité chemikálie - někdy složitý vyvolávací proces
 - úspěšně se používaly ve 2. sv. válce, v některých zemích i po ní

* mikrotečky - fotografie o velikosti tištěné tečky

```
 - tak malá že unikala pozornosti
 - vyvinutá Němci, první odhalena na dopise v r. 1941

* ”Otevřené kódování” neboli ”nulové šifry”
 - skutečná zpráva je kamuflována v nevinně znějící zprávě
 - např. německý špión za 2. sv. války poslal zprávu:

   Apparently neutral’s protest is thoroughly discounted and ignored.
   Ismen hard hit. Blockade issue affects pretext for embargo on
   byproducts, ejecting suets and vegetable oils.

 - ve zprávě každé 2. písmeno slova tvoří skutečnou zprávu: ”Pershing
   sails from NY June 1.”
 - otevřené kódy způsobují určitý ”tón” zprávy => možnost detekce

* postup: objev skryté zprávy => nová metoda

* moderní metody:
 - vysílání v rozptýleném spektru (spread spectrum)
 - drobné posuny slov nebo znaků v dokumentu
 - informace ukrytá do souboru s obrázkem nebo zvukem (modifikace
   nejméně významných bitů - změna je nepostřehnutelná)
  . např. pokud mám obrázek 1024x768 pixelů, každý pixel 3 osmibitová
    čísla RGB => v pixelu 3 bity pro tajnou informaci
  . tj. 1024*768*3 bity = 2 359 296 bitů = 294 912 bytů = 288 KB

* kromě utajené komunikace se dnes se používá zejména pro vkládání
  skrytých ”vodoznaků” do obrázků, digitálně uchované hudby, filmů
  apod.
 - pokud budete prodávat obrázky, které budou mít v sobě tajnou zprávu
   ”Copyright (c) Skutečný Autor” může být problém
 - mělo by vydržet různé transformace => redundance + další schémata

Historické šifry aneb šifrování do II. sv. války
================================================

* český termín ”šifrování” z francouz. chiffre, číslice.
* šifrování má dlouhou a barvitou historii
 . nejstarší primitivní šifry už ve starém Egyptě
 . zde uvedu pouze základní věci jako pozadí moderní kryptografii

* na vývoji šifer se podepsalo hlavně vojenské využití
 - zprávu dostal určený voják, zašifroval, odeslal
 - velké množství zpráv => mnoho obyčejných šifrantů
  . obtížný přechod na jinou metodu (nutno zacvičit velké množství lidí)
  . zároveň ale nebezpečí zajetí šifranta
  . proto metoda parametrizována snadno měnitelným klíčem

Základní model
..............

* základní model vypadá následovně:
 - vstup metody = otevřený text (plaintext) - P
 - transformován šifrovací funkcí parametrizovanou klíčem K
 - výstup šifrovacího procesu = šifrový text (ciphertext), někdy název
   kryptogram - C, C=E_K(P)
 - šifrový text je odeslán (posel, signalizace, rádio...)
 - přijatá zpráva je dešifrována: P=D_K(C)

* protivník = odposlech
 - slyší všechno, zkopíruje si kryptogram C
 - na rozdíl od příjemce nezná K
 - někdy nejen slyší (pasivní odposlech), ale může vkládat vlastní
   zprávy (aktivní odposlech - například komunikaci zaznamená a později
   ji přehraje - playback)
```




```
* věda o návrhu šifer = kryptografie
* luštění šifer = kryptoanalýza
* kryptografie + kryptoanalýza = kryptologie

* jeden ze základních předpokladů - kryptoanalytik zná šifrovací metodu
  (Kerckhoffův princip)
 - vymyslet, otestovat a zavést metodu je tak náročné, že utajení je
   málo pravděpodobné (a není dobré předpokládat že něco není známo když je)
 - dnes předpokládáme masové rozšíření => odposlech může analyzovat šifrovací
   čipy nebo software
 - proto důležitá role klíče = řetězec znaků, který můžeme měnit podle
   potřeby

* výsledný model: veřejně známá metoda parametrizovaná tajným klíčem

* z hlediska odposlechu má problém 3 variace:
 1. odposlech má pouze šifrový text (ciphertext only attack)
 2. odposlech zná část otevřeného textu (known plaintext)
 3. odposlech může nechat zašifrovat vybraný otevřený text (chosen plaintext)

* šifry v zábavné kryptografii by bylo možné rozluštit snadno, pokud
  bychom se mohli zeptat "jak vypadá zašifrované ABCDE?"
 - proto začátečníci v šifrování mylně předpokládají, že postačuje
   odolnost proti ciphertext only útokům
 - v mnoha případech je ale možný "dobrý odhad" části textu (např.
   místo určení, očekávané slovo, obsah polí ve strukturovaných
   zprávách) - vede na known plaintext attack
 - někdy je možné přesvědčit komunikující strany aby přenesly
   požadovaný text - vede na chosen plaintext

* šifra je bezpečná, pokud odolává při libovolném množství vybraného
  otevřeného textu

* historické metody šifrování se v zásadě dělí do 3 kategorií:
 - substituční systémy
 - transpoziční systémy
 - kombinace

Historické metody dovolují i jen pouze ze znalosti šifrového textu
odhalit šifrovací metodu a ekvivalent klíče.

Substituční šifry
.................

* principem je záměna znaku nebo skupiny znaků za jiný znak nebo
  skupiny znaků

* Césarova šifra - nejstarší a nejjednodušší
 - posun o 3 znaky: a bude D, b bude E, c bude F, ..., z bude C
   (malá písmena pro otevřený text, velká pro šifrový text)
 - např. XPLWH WR URCOXVWLW?    (umite to rozlustit?)
 - ve skutečnosti přenášeno např. ve skupinách po 5: XPLWH WRURC OXVWL WZZZZ
 - lehké zobecnění: posun o k => k je klíč
  . k=1  VNJUF UP SPAMVTUJU?
  . k=2  WOKVG VQ TQBNWUVKV?
  . k=3  XPLWH WR URCOXVWLW?
 - všech možných klíčů je 26 => lze vyzkoušet všechny možné klíče
 - prohledání celého prostoru klíčů = útok hrubou silou
```

Uvedená šifra zmátla kdysi Galy, ale pak už asi nikoho. Nicméně ruská carská armáda používala variantu Césarovy šifry ještě za 1. světové války.

* monoalfabetická substituce
 - oproti Césarově šifře podstatné vylepšení - pro každý symbol otevřeného textu mít symbol šifrového textu
 - příklad: a b c d e f g h i j k l m n o p q r s t u v w x y z
            Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
 - např. ”Q RGAQMQSO WNLZT KGMSGXLAFGXZ ZGIST?”
 - možných klíčů je podstatně více: 26! = 4*10^26
 - kdybychom použili hrubou sílu, 1 pokus/1 us => 10^13 let
 - stačí ale poměrně málo šifrového textu, dá se rozluštit s využitím statistických vlastností otevřeného textu:
  . v češtině (ASCII) je nejčastější e, o, a, t, i, n, r, s
  . nejčastější kombinace 2 znaků (bigramy) = st, te, ne, ni
  . trigramy pro, ist, ani
 - analytik nejprve spočte frekvence znaků v šifrovém textu
 - nejčastějším znakům zkusí přiřadit ”e” a ”o”
 - pak hledá trigramy ve formě eXo, X bude pravděpodobně ”h”; pak oYe, Y ~ j atd.
 - postupně může odhalit text; text musí být dost dlouhý, při 26 písmenech je ”dost dlouhý” text > 400 znaků (čím delší tím lepší)

 - v šifrovém textu je možné najít také pravděpodobné slovo nebo frázi
 - např. slovo ’rozlousknout’, má opakující se písmena ’-o--ou---ou-’
 - hledáme vzor: Q RGAQMQSO WNLZT KGMSGXLAFGXZ ZGIST?
                    ok z l   st rozlousknout to l
 - pro vyhlazení statistických charakteristik se do šifrového textu vkládaly tzv. klamače na předem smluvená místa (např. každý 5 znak)

* polyalfabetická substituce
 - použít postupně více abeced; rozšířené díky Vigenérově knize (1586) ”Pojednání o šifrách a tajných způsobech psaní”
 - pro šifrování se používá čtvercová matice 26 Césarových abeced

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
b	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
c	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
d	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
e	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

 - šifrování:
  . klíčem je slovo nebo fráze: napíše se opakovaně nad otevřený text
  . znak otevřeného textu je šifrován podle řádku určeného znakem hesla
  . např: P = prusmyk je zavalen
          K = abcdabc da bcdabcd
          C = QTXWNAN NF BDZBNHR
  . ve skutečnosti součet modulo n: Ci=Pi+Ki (mod 26)
                                    Pi=Ci-Ki (mod 26)
 - analýza:
  . odhadneme délku klíče, vyrobíme tabulku s počtem sloupců = délka klíče
  . do tabulky zapíšeme šifrový text
  . pokud v pořádku, bude mít sloupec stejnou distribuci znaků jako otevřený text => každý sloupec může být řešen jako monoalfabetická šifra

Vigenérovu šifru používali Francouzi od Bonaparta do 1. sv. války; domnívali se, že je nerozluštitelná, Němci jí ale uměli analyzovat.

❇