### Podmínky splnění předmětu

Bude celkem 6 úkolů, cvičení bude virtuální pouze prostřednictvím zadávání a řešení úkolů (zadávány na konci přednášky). Každý by měl odevzdat všechny, je nutné získat alespoň se 60 % bodů.

Na stránce předmětu je literatura, kvalitní je Katz + Lindell – Introduction to Modern Crypto a Goldreich – Foundation of Cryptography vol 1.
Ani jedna z nich není dostupná v elektronické podobě. Proto aby existoval použitelný učební materiál, budeme my dělat zápisy, ty budou korekturovány a zveřejňovány. Za zápis z přednášky není potřeba odevzdat 1 úkol. Zapsané zápisy posílat na adresu *hubacek ⋆at⋆ iuuk.mff.cuni.cz*.

Hlavní část předmětu by mělo být plnění úkolů, deadline bude 2 týdny, na zkoušce si popovídáme o nějakých problémech.

## Foundations of Theoretical Cryptography

### Historie

První zmínky o kryptografii z r. 500 př. n. l., ale až do 2. sv. války byla kryptografie „tajemným uměním“, až za 2. sv války začala být vědou.

Vždy nejprve někdo navrhl systém, někdo jiný na něj navrhl útok, někdo ho opravil a potom se cyklil 2. a 3. bod.

Systém byl považován za bezpečný, pokud ho toho času nikdo neuměl prolomit.

- 1940 – Shannon přišel s rigorózním přístupem ke kryptografii
  - definice perfect secrecy.
  - ukázal, že perfect secrecy je nepraktická.
- 1970 – Diffie a Hellman
  - definice Computational security
  - přišli na to, že nepotřebujeme systémy, které nelze prolomit, stačí, když je nelze prolomit efektivně ⇒ kryptografii lze budovat na obtížných problémech.
  - win-win situace – pokud se podaří prolomit šifru, tak máme alespoň řešení na nějaký obtížný problém.
- 1980 – Goldmasser a Micali
  - „Rozumné“ definice pro kryptografii
  - konstrukce pro dané definice na základě předpokladů jako např. $P \neq NP$, faktorizace je obtížná...
  - Pro to, abychom mohli věřit, že kryptografie existuje, je potřeba věřit, že $P \neq NP$ a většinou je potřeba i nějaký silnější předpoklad.

### Šifrování:

Máme Alici a Boba, kteří by spolu rádi komunikovali, ovšem mají pouze kanál, který odposlouchává Eva (Eavesdropper)

- (realistická situace, postupně existovali kurýři, pošta, email, mobil...)
- „encryption scheme“/secret code/secret key
- dříve fungovala Stegamografie – způsob, jak schovat data do jiné legitimně vypadající zprávy, v dnešní době ale tento přístup již není zajímavý.

**Public-key cryptography**

- bez sdíleného klíče
- autentizace a integrita dat
  - Alice ověří zprávu od Boba (může si být jistá, že zpráva je opravdu od něj a nebyla modifikována)
- Mimo komunikaci: secure computation
  - protokoly pro aukce, e-cash, voting, kdy máme mnoho účastníků, adversary je interní – chceme docílit toho, aby nikdo např. nemohl ovlivnit volby mimo váhu vlastního hlasu.

**Vrstvy kryptografie**

1. Výpočetně složité problémy
   - základní stavební kameny
   - vycházejí z teorie složitosti nebo z výpočetní teorie čísel (v některých grupách diskrétní logaritmus, faktorizace,. . . )
   - nutné předpoklady:
   - u Shannona – šifry použitelné, i když má Eva neomezenou výpočetní sílu. Zde nám ale stačí předpoklad, že náš problém je obtížný (nevíme ale, jestli nějaký takový opravdu existuje)
2. Kryptografická primitiva
   - základní „kryptografický úkol“ – šifrování, digitální podpis, pseudonáhodné generátory, zero-knowledge proof
   - konstrukce s důkazy bezpečnosti
3. Protokoly
   - aukce, voting,
   - též máme důkazy bezpečnosti, ale většinou se pouze odkazují na důkazy předchozí vrstvy
4. Systémy
   - TLS/SSL – důkazy bezpečnosti většinou ještě neexistují, též jsou ale typicky nutné dobré stavební prvky z předchozích vrstev.

**Private-key Encryption (Symetric)**

Alice a Bob mají sdílený klíč Předpoklady:

- Kerchhoffův princip: Předpokládáme, že encryption i decription algoritmy jsou známé, adversary nezná klíč. (dobrý předpoklad, algoritmy vždycky nakonec uniknou)
- insecure channel – adversary vidí všechny správy, ale je pasivní (nemůže měnit, ničit, či tvořit vlastní zprávy)

**Definice:** *Private-key encryption scheme* s prostorem klíčů $\mathcal{K}$, prostorem zpráv $\mathcal{M}$ a prostorem ciphertextů $\mathcal{C}$ je trojice algoritmů $(G, E, D)$, kde:

- $G$ generuje klíče z $\mathcal{K}$, značíme $k \leftarrow G$, $k \in \mathcal{K}$
- $E$ pro klíč $k \in \mathcal{K}$ a zprávu $m \in \mathcal{M}$ vrací ciphertext $c \in \mathcal{C}$, značíme $c \leftarrow E_k(m)$.
- $D$ pro klíč $k \in \mathcal{K}$ a cipher text $c \in \mathcal{C}$ vrací zprávu $m$, značíme $m = D_k(c)$.

Šipky v definicích znamenají, že $G$ a $E$ není deterministický ale pravděpodobnostní, $D$ je naopak deterministický (to nás neomezuje, tyto případy se na sebe dají převést)

Požadujeme korektnost, tedy $\forall k \in \mathcal{K}, m \in \mathcal{M}, D_k(E_k(m)) = m$.

Typicky $|\mathcal{M}| \neq |\mathcal{C}|$.

Co od algoritmu chceme v rámci bezpečnosti - požadovat, aby ciphertext nic neříkal o klíči nefunguje.

**Definice:** Private-key encryption scheme splňuje *perfect indistinguishability*, pokud $\forall m_1, m_2 \in \mathcal{M}, c \in \mathcal{C} : Pr_{k\leftarrow\mathcal{K}}[E_k(m_1) = c] = Pr_{k\leftarrow\mathcal{K}}[E_k(m_2) = c]$, pravděpodobnost počítáme přes pravděpodobnost $k \leftarrow G$ a náhodné mince v $E$.

Pokud jsme schopní splnit tohle, znamená to, že adversary z ciphertextu opravdu nezjistí vůbec nic, dokonce i kdyby znal část zprávy (klidně celou až na jeden bit).

**Příklad:** Shift cipher (Caesarova šifra) $\mathcal{K} = \{0, 1, \ldots, 25\}$,$\mathcal{M} = \mathcal{C} = \mathcal{K}^\ell$ Substitution cipher $K = \Phi(25)$ (=permutace na $\{0, 1, \ldots, 25\}$), $\mathcal{M} = \mathcal{C} = \mathcal{K}^\ell$ One-time pad(Vernamova šifra) $\mathcal{K} = \mathcal{C} = \mathcal{M} = \{0,1\}^\ell$ $E_k(m) = m \oplus k$, $D_k(m) = m \oplus k$

**Tvrzení:** Caesarova šifra pro zprávy délky $\ell \geq 2$ nesplňuje perfect ind.

**Důkaz:** $m_1 = aa$, $m_2 = ab$, $c = xy$, $Pr_{k\leftarrow\mathcal{K}}[E_k(m_2) = c] = \frac{1}{26}$ $Pr_{k\leftarrow\mathcal{K}}[E_k(m_1) = c] = 0$ □

**Tvrzení:** OTP splňuje perfect ind.

**Důkaz:** $Pr_{k\leftarrow\mathcal{K}}[E_k(m) = c] = Pr_{k\leftarrow\mathcal{K}}[n = m \oplus c | k \leftarrow \{0,1\}^\ell] = 2^{-\ell}$ □

**Definice:** $M$ je pravděpodobnostní rozdělení na $\mathcal{M}$. Pak PK encryption scheme splňuje *Shannon secrecy* vzhledem k $M$, pokud $\forall m \in \mathcal{M}, c \in \mathcal{C}$ taková, že $Pr[E_k(m) = c] > 0$ platí $Pr[M = m | E_k(m) = c] = Pr[M = m]$

Pravděpodobnost přes $M$, $k \to \mathcal{K}$ a $E$.

**Tvrzení:** PK-encryption scheme splňuje perf. ind. právě když splňuje Shannon secrecy (vzhledem ke každému $M$, $Pr[M = m] > 0 \forall m \in M$) Pak říkáme, že splňuje perfect secrecy.

**Důkaz:** "⇒"

Bayesova věta: Pokud platí $Pr[B] > 0$, pak $\forall A$ :

$$Pr[A|B] = \frac{Pr[B|A]Pr[A]}{Pr[B]}.$$

Z Bayesovy věty platí

$$Pr[M = m | E_k(m) = c] = \frac{Pr[E_k(m) = c | M = m]Pr[M = m]}{Pr[E_k(m) = c]}.$$

Z perf. ind. ale platí, že $Pr[E_k(m) = c | M = m] = Pr[E_k(m) = c]$, tyto členy můžeme proti sobě tedy pokrátit a dostaneme $Pr[M = m | E_k(m) = c] = Pr[M = m]$, čímž je tato implikace dokázána.

Zbytek důkazu na příští přednášce.