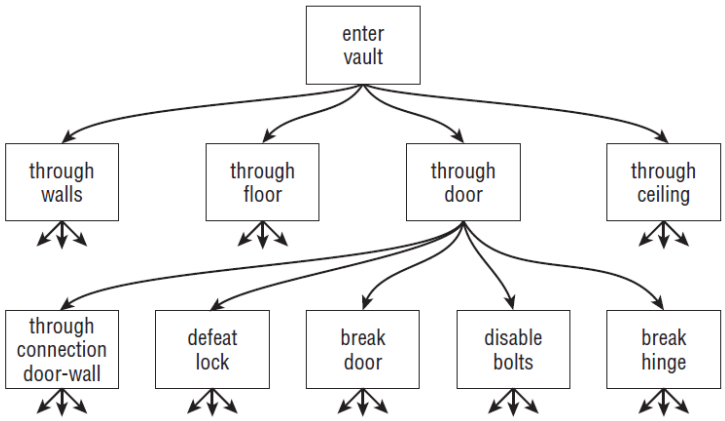
1. “A security system is only as strong as its weakest link” Abychom zlepšili bezpečnost systému, musíme zlepšit nejslabší článek. K tomu však potřebujeme vědět, jaké jsou tyto články a které z nich jsou slabé. Toho můžeme např. Dosáhnout pomocí hierarchické stromové struktury.



   a) Vytvořte strom útoku pro zjištění jména a hesla k online bankovnímu účtu jiné osoby.
   b) Vytvořte strom útoku pro čtení e-mailů jiné osoby.
   c) Vytvořte strom útoku pro zabránění jiné osobě ve čtení jejích vlastních e-mailů.

2. Kerckhoffův princip. Uveďte alespoň dva argumenty pro Kerckhoffův princip a alespoň dva argumenty proti Kerckhoffovu principu. Poté uveďte a zdůvodněte svůj názor na platnost Kerckhoffova principu.

3. Navrhněte 2 jakékoliv způsoby utajení obsahu textu M. Popište postup pro transformaci na text „nečitelný“ a zpět (tedy pro převedení zpět na text čitelný, srozumitelný). Tedy vymyslete mechanismus pro zajištění utajení (důvěrnosti, confidentiality) zadaného textu. Nechci žádný existující algoritmus (byť inspirovat se můžete). Stačí slovní popis postupu a definice přípustných operací a hodnot. Postup si zaznamenejte. M = Dnes je první den letního semestru. Přeji Vám mnoho zdaru!

4. Předpokládejme, že Alice a Bob si navzájem posílají e-maily přes internet. Tyto e-maily posílají ze svých notebooků, které jsou připojeny k free wifi sítím poskytovaným jejich oblíbenými kavárnami. Uveďte všechny strany, které by mohly tento systém napadnout, a co by mohly dosáhnout. Popište, jak by se Alice a Bob mohli bránit proti každému z útoků, které jste výše identifikovali.