0. Pojmy

Vysvětlete lidsky jednou větou, co to je nebo co to dělá:

- Kontrolní součet
- Hashovací funkce
- Symetrická šifra
- Asymetrická šifra
- Digitální podpis

Cvičení 1a: kontrola vůči zpřeházení

Nejčastějším překlepem je prohození dvou sousedních písmen. Jaký kontrolní součet použít?

Cvičení 2a: lámání hesel

Operační systém ověřuje, jestli uživatel zadal správně heslo. Útočník může číst všecha data z disku. Útočník nesmí odhalit hesla.

1. Útočník si může předem připravit libovolně náročný výpočet.
2. Chceme, aby systém sloužil dlouhodobě, přestože se počítače neustále zrychlují.

Cvičení 2b: vzdálené přihlášení

Server ověřuje, jestli uživatel zadal správně heslo. Útočník vidí všechny zprávy. Útočník se nesmí přihlásit – přestože může poslat doslova totéž, co dřív posílal uživatel.

Cvičení 2c: kámen, nůžky, papír

Uživatelé si chtějí po sítí náhodně vylosovat, kdo vyhrál. Síť je bezpečná, ale oba můžou podvádět.

1. Protokol může selhat, pokud uživatelé nespolupracují.
2. Pokud protokol neselže, tak oba musejí mít záruku, že výsledek je spravedlivý.

Cvičení 2d: anonymní dotazník

Studenti vyplňují dotazník ohledně výuky. Chceme zajistit, že každý ho vyplní jednou.

1. Z našich záznamů nesmí jít zjistit, kdo odpovídal jak.
2. Když program spouštíme, měl by obsahovat co nejmíň dat. Nechceme si ukládat přihlašovací údaje.

Cvičení 3a: hashovací funkce pomocí šifry

Máme k dispozici program na symetrické šifrování a chceme vyrobit program na hashovací funkci. Dává naše řešení patřičné záruky? Jaké má nevýhody oproti skutečné hashovací funkci?

Cvičení 3b: šifra na jedno použití

Potřebujeme si zajistit šifrovanou komunikaci s ponorkou po celou dobu jejího provozu. Ponorce můžeme jednou bezpečně předat data, a to když vyplouvá z přístavu.

1. Útočník má k dispozici neomezený výpočetní výkon.

Cvičení 3c: šifrování wi-fi

Zabezpečení WEP se sdíleným klíčem spoléhá na to, že uživatelé znají klíč a útočník nikoli.

1. Pokud uživatelé pošlou dvakrát úplně stejnou zprávu, útočník to nesmí poznat.

Cvičení 4a: end-to-end šifrování

Uživatelé chtějí komunikovat v prostředí, kde útočník může kteroukoliv zprávu přečíst nebo změnit. Pokud útočník zprávu změní, protokol musí

selhat a zprávu nedoručit. Pokud protokol neselže, útočník se nesmí dovědět skoro nic o obsahu zprávy.

1. Jak takový protokol implementovat pomocí asymetrické šifry?
2. Co se útočník o zprávě dozví nevyhnutelně?

Cvičení 4b: útok CRIME

Představme si následující protokol:

1. Uživatel pošle serveru požadavek obsahující libovolný kód M.
2. Server na konec kódu M připíše tajnou zprávu S, obojí zkomprimuje, zašifruje tajným klíčem a výsledek pošle zpět.
3. Uživatel zná tajný klíč, takže přijatá data dešifruje, rozbalí zip a přečte zprávu S.

Útočník může serveru poslat požadavek kolikrát chce a zpráva S je pořád stejná. Útočník nezná tajný klíč. Jak může odhalit zprávu S?

Cvičení 4c: symetrická šifra pomocí asymetrické

Máme k dispozici všechny tři programy na asymetrické šifrování a chceme vyrobit program na symetrické šifrování. Naše zadání to neumožňuje vyřešit. Kde je potíž?

Cvičení 4d: rychlejší asymetrické šifrování

Asymetrické šifryjsou moc pomalé na zpracování velkých objemů dat. Jak zaručit bezpečí asymetrické šifry a rychlost té symetrické?

Cvičení 5a: podpis zprávy

Uživatelé se můžou jednou potkat a bezpečně si předat libovolná data. Později si chtějí poslat e-mail. Útočník může zprávu přečíst a změnit.

1. Pokud útočník zprávu změní, protokol musí selhat.
2. Digitální podpis je moc pomalý na zpracování celé zprávy.

Cvičení 5b: řetěz certifikátů

Chceme ověřit, že se připojujeme na správný webový server. Na celém světě jsou tisíce důvěryhodných advokátů, kteří se osobně setkají s majitelem serveru a vystaví mu certifikát.

1. Jak označovat důvěryhodné advokáty?
2. Pracovní zátěž se nesmí v systému soustředit na jedné osobě.
3. Občas některému advokátovi přestaneme důvěřovat.

Cvičení 5c: síť důvěry

Uživatel, kterého jsme doteď neznali, nám pošle e-mail. Chceme ověřit, že zprávu poslal on.

1. Máme společné kamarády.
2. Nemáme společné kamarády, ale naši kamarádi se mezi sebou znají.

Cvičení 5d: podpis fotografie

Fotoaparát v sobě může mít bezpečně uložené tajemství, a veřejně (i útočníkovi) dávat svoje ověřovací údaje. Chceme mít možnost ověřit, že fotografie byla vyrobená na daném fotoaparátu.

Cvičení 5e: vodoznak

Fotoaparát v sobě má uložené tajemství, které je známé jen jeho výrobci. Vodoznak je strojově čitelný údaj nenápadně zabudovaný do každé fotografie, který obsahuje číslo fotoaparátu. Útočník musí mít jen malou šanci vodoznak smazat a nepoškodit přitom celý obraz.

Demotivační cvičení: problém milionářů

Dva milionáři chtějí zjistit, kdo je bohatší. Měsíční výdělek každého z nich je celé číslo v rozsahu 0 a 10^9 dolarů.
Máme zaručit:

1. Nedovědí se *nic víc* o tom, kolik peněz vydělává ten druhý.
2. Jeden i druhý milionář může podvádět. Protokol v takovém případě smí dát špatný výsledek (samozřejmě), ale nesmí odhalit nic navíc.