

PV178 Úvod do vývoje v C#/.NET

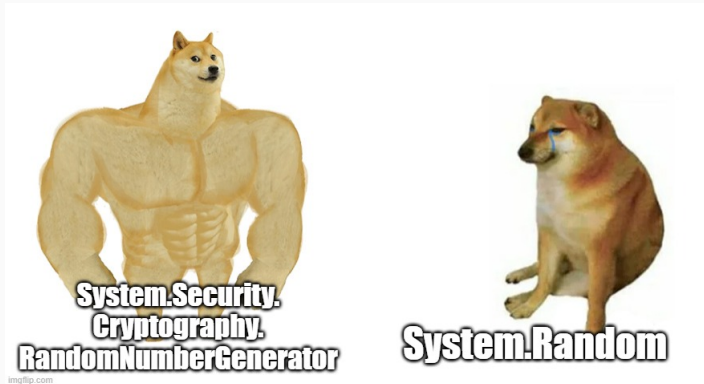
Cvičenie 12

Fakulta informatiky, Masarykova univerzita, Brno

- náhodné čísla
- hashovanie
- ukladanie hesiel
- symetrické šifrovanie
- asymetrické šifrovanie

Náhodné čísla

- dôležité pre generovanie šifrovacích kľúčov



- väčšia bezpečnosť, pomalší výkon

Hashovanie

- hashovacia funkcia berie na vstupe správu a vracia dáta (hash) s pevnou dĺžkou
- hash má nasledujúce vlastnosti:
 - dá sa vygenerovať z hocijakej správy
 - nie je možné z nej vygenerovať vstupnú správu
 - zmení sa pri zmene vstupnej správy
 - nie je možné nájsť dve odlišné správy s rovnakým hashom
- kontrolujeme tým integritu dát

Task 1: SHA256

- Vytvorte metódu, ktorá bude hashovať zadaný string pomocou algoritmu SHA256 a vypíše výsledný hash do konzoly.

HMAC

- hash skombinovaný s tajným klúčom
- kontrolujeme tým aj autenticitu dát

Ukladanie hesiel

- ako neukladať heslá?
 - otvorený text – instant win
 - hash hesla – brute force alebo dictionary útok
 - šifrovanie hesiel – kam dám kľúč?

Ukladanie hesiel

- ako neukladať heslá?
 - otvorený text – instant win
 - hash hesla – brute force alebo dictionary útok
 - šifrovanie hesiel – kam dám kľúč?
- ako ukladať heslá?
 - hash hesla a náhodnej salt – nepomôže mi predpočítaná hash častých hesiel, keďže dve rovnaké heslá budú mať iný hash + brute force bude dlhšie trvať
 - password based key derivation function – ako input pridáva počet iterácií hashovania hesla a náhodnej salt
 - salt a počet iterácií nemusia byť tajné hodnoty

Task 2: Hacking

- Vymyslite si krátky pin zložený len z číslic (napr. 421337). Porovnajete rýchlosť úspešného brute force útoku pre tieto prípady uloženého pinu:
 - otvorený text,
 - MD5 hash,
 - SHA512 hash,
 - heslo zahashované cez PBKDF2 s 16 bytovou soľou a 20 iteráciami.

Symetrické šifrovanie

- jedným kľúčom šifrujeme aj dešifrujeme
- bezpečné, rýchle
- čo ale s kľúčom?

Asymetrické šifrovanie

- rieši problém "čo s kľúčom?"
- private a public kľúč – jeden šifruje, druhý dešifruje
- verejný kľúč je... verejný... a žiadne tajomstvo sa nemusí zdieľať
- pomalšie v porovnaní so symetrickým šifrovaním
- algoritmy často využívajú modulárnu aritmetiku a prvočísla