

Organizační informace

Tématická náplň, organizace, hodnocení

Milan Radojčić

SSPŠaG – KBB

7. listopadu 2025



Tématická náplň

1. Matematické základy, algebra, teorie čísel
2. Historické šifry
3. Asymetrická kryptografie, Diffieho-Hellmanova výměna klíčů, RSA
4. Proudové šifry, one-time pad, RC4, ChaCha20
5. Blokové šifry, DES, AES
6. Hašovací funkce
7. Infrastruktura veřejného klíče
8. Bezdrátové sítě; Útoky postranními kanály
9. Post-quantová a kvantová kryptografie
10. Architektura x86, assembler
11. Binary exploitation, reversing



Hodnocení

- ▶ bodový systém
 - 100 bodů za pololetí
- ▶ 2 menší testy z matematických základů
- ▶ 2 testy z kryptografie
- ▶ implementace šifry
- ▶ větší úkol na assembly
- ▶ **bonusové kvízy, úlohy a body za aktivitu¹**
- ▶ **bonusové body za nalezení chyb v materiálech²**

Body	Známka
100-90	1
89-75	2
74-60	3
59-45	4
44-0	5

Tabulka: Převod bodů na známku

¹max. 10 bodů za pololetí

²max. 5 bodů za pololetí



- ▶ Presentace, skripta a příklady k procvičení budou na <https://radojcic.cz/kbb>.
- ▶ Můžou se hodit následující knihy:
 - Simon Singh: *Kniha kódů a šifer*. 1999³
 - Karel Burda: *Úvod do kryptografie*. 2015
 - M. Mareš, T. Valla: *Průvodce labyrintem algoritmů*. 2017⁴

³V originále *The Code Book*.

⁴Dostupné z <https://pruvodce.ucw.cz>.

