Skúška z predmetu Aplikovaná kryptografia ZS 2018

Test, 20 otázok (Áno/Nie) - **20 bodov**

Písomná časť, 4 otázky z okruhu - **30 bodov**

Obhajoba zadania - **10 bodov**

Okruhy otázok na písomnú časť z predmetu Aplikovaná kryptografia

1. Algoritmus AES
2. Generátory náhodných čísel
3. Režimy blokových šifier
4. Algoritmus RSA
5. Galoisove polia a ich využitie v kryptografii
6. Algoritmus na výmenu kľúčov Diffie-Hellman
7. Eliptické krivky
8. Hašovacie funkcie
9. Autentifikačný kód správy MAC
10. Digitálne podpisy