

POKR – TEMATYKA NA ĆWICZENIA

1. Charakterystyka podpisu cyfrowego przy użyciu różnych algorytmów szyfrujących.
2. Sposoby zapewnienia usługi poufności.
3. Sposoby dystrybucji kluczy.
4. Dystrybucja klucza tajnego Diffiego-Hellmana z usługą integralności.
5. Opracowanie zadań do ataku na szyfry klasyczne.
6. Ataki Man in The Middle.
7. Rodzaje szyfrów strumieniowych.
8. Szyfry blokowe.
9. Kerberos.
10. Telnet i SSH.
11. SSL.
12. IPSec.
13. PGP/GPG – usługi kryptograficzne.
14. Współczesna steganografia.
15. Działanie zapór ogniowych.
16. Szyfrowanie z uwierzytelnieniem.
17. Cryptool – usługi kryptograficzne.
18. Protokół Needhama-Schroedera.