**Przedmiot:** Systemy operacyjne

**Tematyka:** Bezpieczeństwo

**Wybierz dwa z podanych czterech zadań.**

**Zadanie 1.** Szyfrowane połączenie - jeśli za trudne, przejdź do Zadania 3.

Rozbuduj swój program chat z zadania IPC. Korzystając z bibliotek udostępniających funkcjonalność szyfrowania (np. openssl) dodaj opcję szyfrowania do swojego kodu.

Zaprezentuj z użyciem programu tcpdump lub wireshark różnice w poufności.

**Zadanie 2.** Zakleszczenie i zagłodzenie

Rozważ zakład produkcyjny:

* zakład produkuje P różnych produktów: Produkt\_1, Produkt\_2, … Produkt\_P,
* do produkcji wykorzystuje M różnych materiałów: Materiał\_1, Materiał\_2, … Materiał\_M,
* produkcja odbywa się na S różnych maszynach, Maszyna\_1, Maszyna\_2, … Maszyna\_S,
* zatem każdy produkt można opisać wektorem użytych materiałów, na przykład: [ 5, 0, 6, 3, 0 ], co oznacza że przykładowy produkt wymaga 5 jednostek materiału pierwszego, nie potrzebuje materiału drugiego, 6 jednostek materiału trzeciego, itd.
* oraz podobnie, każdy produkt można opisać wektorem użytych maszyn, j.w. (za wyjątkiem takim, że wartości współrzędnych tego wektora mogą przyjmowac tylko 0 lub 1).
* produkcja każdego z produktów trwa pewną ilość jednostek czasu wynoszącą C[Produkt\_X],
* zakład ma dwa magazyny: magazyn materiałów o pojemności MM i magazyn produktów o pojemności PP,
* transport materiałów z magazunu oraz produktów do magazynu trwa zero jednostek czasu,
* materiały dostarczane są do magazunu materiałów w pewnej losowej ilości każdy w pewnych losowych odstępach czasu,
* produkty pobierane przez klientów z magazynu są w pewnej losowej ilości każdy w pewnych losowych odstępach czasu.

Napisz program, który dla zadanych wartości:

* parametrów: P, M, S,
* wektorów: materiałów, maszyn, czasu,
* pojemności: MM i PP,

zoptymalizuje działanie tak, aby:

* w magazynie produktów zawsze był przynajmniej jeden produkt każdego rodzaju.

**Zadanie 3.** Instrukcja 06-SO-Bezpieczenstwo.pdf

**Zadanie 4. Szyfrowany system plików**

Zaszyfruj plik losowy.dat, załóż na nim system plików i zamontuj w systemie.

Podpowiedź: cryptsetup (luksFormat, luksOpen/open, luksClose/close).

Proszę obserwować pojawianie się urządzenia w: /dev/mapper/

Rozszerzenie: przygotować działanie tego zadania tak, aby klucz szyfrujący znajdował się na pendrive i po jego włożeniu następowało automatyczne odszyfrowanie i zamontowanie (podpowiedź: pliki /etc/crypttab i /etc/fstab).

Czy zaszyfrowany system plików w przypadku uszkodzenia fizycznego pozawala na dostęp do danych ?