POLITECHNIKA BIAŁOSTOCKA
WYDZIAŁ INFORMATYKI
Bezpieczeństwo sieci komputerowych

PRACOWNIA SPECJALISTYCZNA 6-7
DR INŻ. MACIEJ BRZOZOWSKI

TEMAT: KRYPTOSYSTEMY SYMETRYCZNE - ALGORYTM DES.

Zadania: Wykonaj program realizujący szyfrowanie oraz deszyfrowanie z wykorzystaniem algorytmu DES. Więcej informacji w dokumencie źródłowym **fips46-3**.

Punktacja (maksymalnie 9 punktów):

1. generowanie kluczy 2 pkt.
2. funkcja $f(R, k)$ 2 pkt.
3. kolejki 2 pkt.
4. złączenie w całość komponentów kluczy, funkcji oraz kolejek 1 pkt.
5. padding informacji przy szyfrowaniu i rozszyfrowaniu 1 pkt.
6. obsługa plików binarnych 1 pkt.

Testy:

- `http://dhost.info/pasjagor/des/start.php`
- `http://people.eku.edu/styere/Encrypt/JS-DES.html`