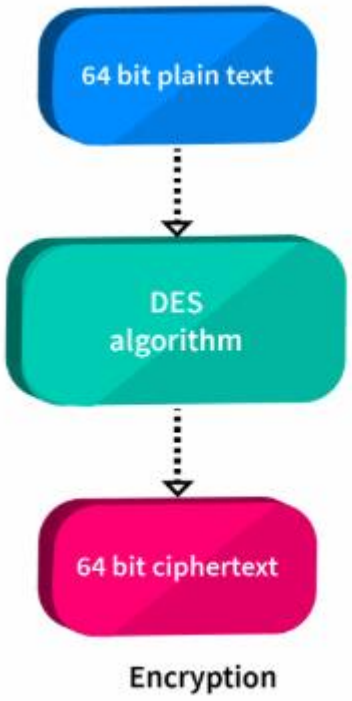
DES

DES

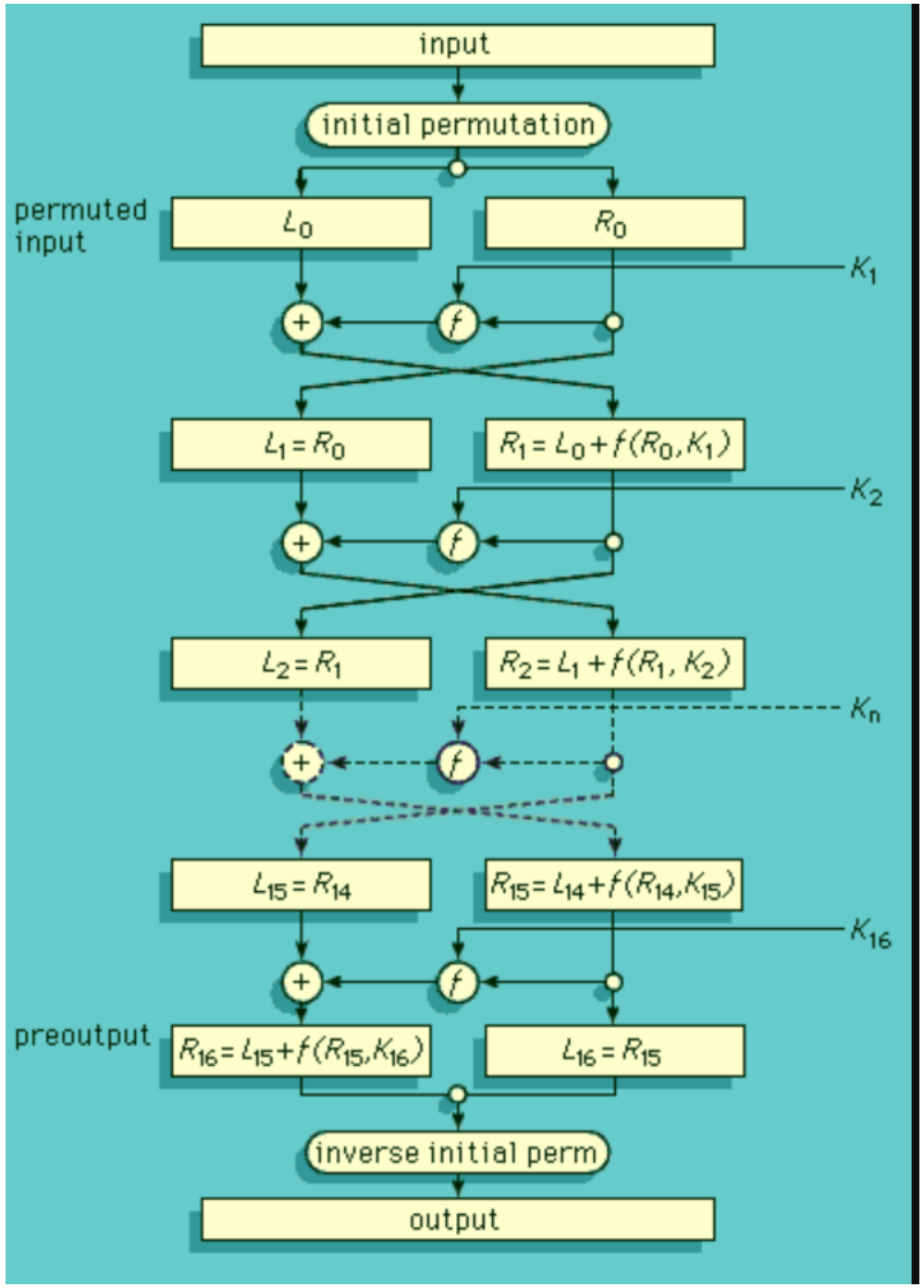


- **DES** – אלגוריתם הצפנה סימטרי

- **גודל בלוק:** 64 ביט (8 בתים)
אם הטקסט לא מתחלק ל-64 ביט ⇒ צריך להשתמש ב־**padding**.

- **גודל מפתח:** 64 ביט (רק **56 ביטים** משמשים בפועל)
- **מספר סיבובים:** 16 סיבובים
- **שיטת עבודה:** מבוסס על מבנה **Feistel**

DES



שלב אתחול – פרמוטציה של הודעת מקור. כל ביט יוחלף עם ביט אחר

פונקציה F –

הרחבת 32→48 ביט

XOR עם תת־מפתח

תיבות S (S-boxes)

פרמוטציה

DES3

Triple DES (3DES)

אלגוריתם הצפנה סימטרית הבנוי מ-3 פעולות DES ברצף:

- הצפנה עם מפתח ראשון K1
- פענוח עם מפתח שני K2
- הצפנה שוב עם מפתח שלישי K3

- אם $K1 = K2 = K3 \Rightarrow$ מצב של DES
  אם $K1 \neq K2 \neq K3 \Rightarrow$ מצב Triple DES (מאובטח יותר)

DES3

- Padding
- כאשר הנתונים אינם בגודל 8 בתים – נצטרך להרחיב אותם.

```
Plaintext: "HELLO"
ASCII:     72 69 76 76 79          ← 5 בתים
Padding:   03 03 03                ← כי חסרים 3 בתים
```

DES3

- הצפנה

```
C = E_K3(D_K2(E_K1(P)))
```

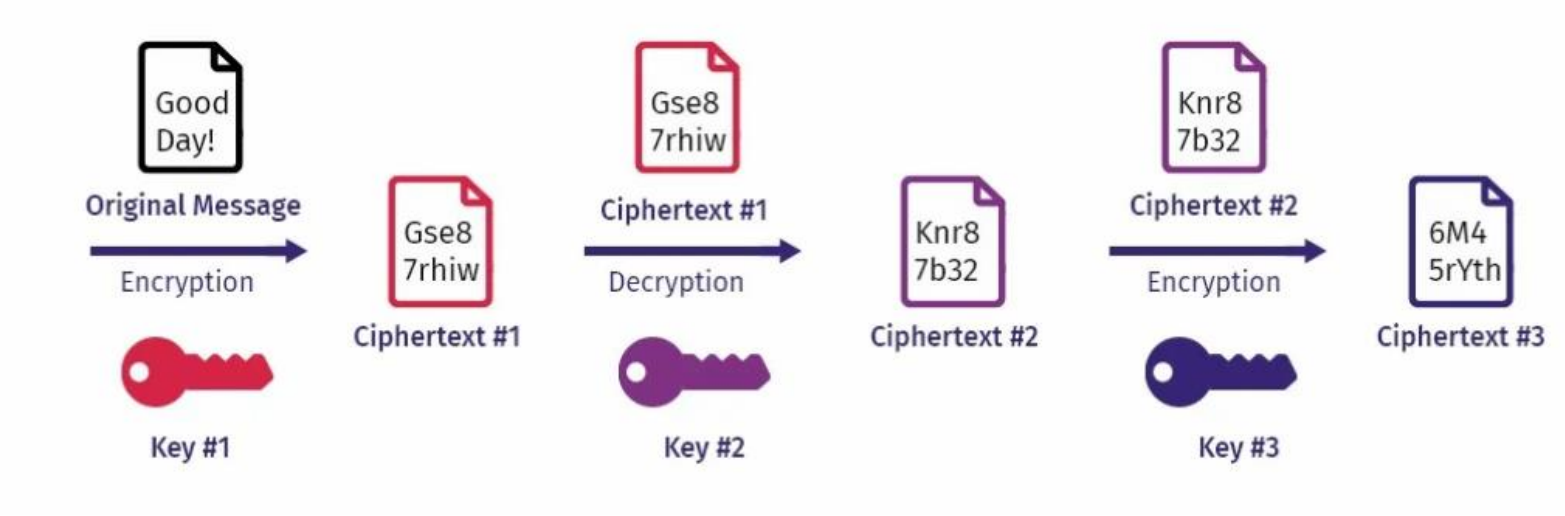
הצפנה עם מפתח 1

פענוח עם מפתח 2

הצפנה עם מפתח 3

-

```
for block in blocks:
    block = des_encrypt(block, key1)
    block = des_decrypt(block, key2)
    block = des_encrypt(block, key3)
    ciphertext += block
```



DES3

- פענוח

```
P = D_K1(E_K2(D_K3(C)))
```

פענוח עם מפתח 3

הצפנה עם מפתח 2

פענוח עם מפתח 1

```
for block in blocks:
    block = des_decrypt(block, key3)
    block = des_encrypt(block, key2)
    block = des_decrypt(block, key1)
    plaintext += block
```

DES3

תרגיל – מימוש DES3

- יש לקבל קלט מחרוזת מהמשתמש.
- להמיר ל-ASCII ולהוסיף padding לפי הצורך.
- יש לבצע הצפנה Triple DES לפי שלושת המפתחות.
- יש להדפיס פלט של ההצפנה בפורמט HEX.
- יש לבצע פענוח ולהדפיס את הטקסט המקורי.