

i dont understand this slide please briefly write each point then explain it without too much details\



Here's a brief explanation of each point on the slide:

slide 94

1. An initial permutation before round 1:

- This means that before any encryption rounds start, the bits of the plaintext are rearranged according to a specific pattern.
- Purpose: It's mainly for historical reasons and not for added security.

2. Halves are swapped after the last round:

- After all encryption rounds, the left and right halves of the data are swapped.
- Purpose: This is part of the encryption structure but doesn't increase security directly.

3. A final permutation (inverse of initial perm) applied to (R16, L16):

- After the halves are swapped, the inverse of the initial permutation is applied to get the final ciphertext.
- Purpose: It reverses the initial permutation, making the process reversible for decryption.

4. None of this serves security purpose:

- These steps (initial/final permutation and swapping) do not directly make the encryption more secure.
- They were likely included to make hardware implementation simpler when DES was created.

The initial and final permutations, along with the swapping of halves, are structural elements of the DES algorithm but don't add to its cryptographic strength.

🔊 📄 👍 🗨️ ↺ ▾



Message ChatGPT

