Hệ thống kiểm tra trùng lặp nội dung

KẾT QUẢ KIỂM TRÙNG TÀI LIỆU

THÔNG TIN TÀI LIỆU

Tên tác giả:	HUIT 50
Tên file:	KLKS DES ATTT2025.pdf
Thời gian nộp:	10/06/2025 03:21:51
Thời gian trả kết quả:	10/06/2025 03:23:13
Chế độ kiểm tra:	Việt - Việt
Số trang:	95
Số câu:	484
Số câu tương đồng:	7
Mức độ cảnh báo:	THẤP (cao: > 15%; trung bình: 2÷15%; thấp: < 2%)

KẾT QUẢ KIỂM TRA TRÙNG LẶP

Độ tương đồng:

1.45%	**0.00%**	**1.24%**	**0.62%**
Trên tất cả tài liệu	Trên tài liệu nội bộ của trường	Trên tài liệu nội bộ của trường khác	Từ nguồn Internet

Nguồn trùng lặp nhiều nhất: 0.826%

Tài liệu hệ thống - Tìm hiểu kỹ thuật mã hóa DES trong hệ thống bảo mật thông tin.txt

Các loại trừ:
- Các nội dung trước lời nói đầu, lời mở đầu.
- Các câu ít hơn 7 từ.

Kết quả kiểm trùng với tài liệu: Tài liệu hệ thống - Tìm hiểu kỹ thuật mã hóa DES trong hệ thống bảo mật thông tin.txt

Tỉ lệ sao chép: **0.826%**

Trang	Chỉ số	Tài liệu kiểm tra	Tài liệu gốc
x	1	Sơ đồ quá trình sinh khóa con (1) Bảng dịch bit của 16 vòng khóa con như sau: Vòng 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 Số bit dịch 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1 Bảng 3.4	vòng lặp 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 số bít dịch 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1 bảng 2.4: bảng dịch bit tại các vòng lặp của des ki = pc-2(cidi)
x	2	Bảng hoán vị khởi tạo đầu và cuối (IP, IP-1) như sau: Bảng IP 58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4 62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8 57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3 61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7 Bảng 3.5	phép hoán vị ip thực hiện dựa trên các bảng sau, với các giá trị trong bảng cho biết số thứ tự của bit trong khối thông tin (từ 1 đến 64) : 58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4 62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8 57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3 61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7 bảng 2.1: bảng hoán vị ip 64 bít trong khối thông tin (m1, m2, …, m64) được ánh xạ vào các vị trí tương ứng trong bảng hoán vị ip, sau đó được đọc ra tuần tự theo từng dòng từ trên xuống
x	2	Bảng hoán vị khởi tạo đầu và cuối (IP, IP-1) như sau: Bảng IP 58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4 62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8 57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3 61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7 Bảng 3.5	40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31 38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29 36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27 34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25 bảng 2.2: bảng hoán vị ngược ip-1 lưu ý rằng hai hoán vị ip và ip-1 không có ý nghĩa gì về mặt mật mã mà chỉ tăng thêm tính phức tạp đồng thời nhằm tạo điều kiện cho việc “chip hóa” thuật toán des
x	2	Bảng hoán vị khởi tạo đầu và cuối (IP, IP-1) như sau: Bảng IP 58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4 62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8 57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3 61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7 Bảng 3.5	57 49 41 33 25 17 9 1 58 50 42 34 26 18 10 2 59 51 43 35 27 19 11 3 60 52 44 36 63 55 47 39 31 23 15 7 62 54 46 38 30 22 14 6 61 53 45 37 29 21 13 5 28 20 12 4 bảng 2.3: bảng trật tự khóa pc-1 64 bít khóa ban đầu được chọn lấy 56 bít theo quy tắc đã nói ở trên, sau đó được đưa vào khối hoán vị pc-1
x	3	Bảng hoán vị IP và IP-1 Bảng IP-1 40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31 38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29 36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27 34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25	phép hoán vị ip thực hiện dựa trên các bảng sau, với các giá trị trong bảng cho biết số thứ tự của bit trong khối thông tin (từ 1 đến 64) : 58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4 62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8 57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3 61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7 bảng 2.1: bảng hoán vị ip 64 bít trong khối thông tin (m1, m2, …, m64) được ánh xạ vào các vị trí tương ứng trong bảng hoán vị ip, sau đó được đọc ra tuần tự theo từng dòng từ trên xuống

x	3	Bảng hoán vị IP và IP-1 Bảng IP-1 40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31 38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29 36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27 34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25	40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31 38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29 36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27 34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25 bảng 2.2: bảng hoán vị ngược ip-1 lưu ý rằng hai hoán vị ip và ip-1 không có ý nghĩa gì về mặt mật mã mà chỉ tăng thêm tính phức tạp đồng thời nhằm tạo điều kiện cho việc “chip hóa” thuật toán des
x	3	Bảng hoán vị IP và IP-1 Bảng IP-1 40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31 38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29 36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27 34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25	57 49 41 33 25 17 9 1 58 50 42 34 26 18 10 2 59 51 43 35 27 19 11 3 60 52 44 36 63 55 47 39 31 23 15 7 62 54 46 38 30 22 14 6 61 53 45 37 29 21 13 5 28 20 12 4 bảng 2.3: bảng trật tự khóa pc-1 64 bít khóa ban đầu được chọn lấy 56 bít theo quy tắc đã nói ở trên, sau đó được đưa vào khối hoán vị pc-1
x	4	33 Bước 1: Khóa gốc sẽ được đi qua bảng hoán vị PC-1 Bảng PC-1 57 49 41 33 25 17 9 1 58 50 42 34 26 18 10 2 59 51 43 35 27 19 11 3 60 52 44 36 63 55 47 39 31 23 15 7 62 54 46 38 30 22 14 6 61 53 45 37 29 21 13 5 28 20 12 4 Bảng 3.6	57 49 41 33 25 17 9 1 58 50 42 34 26 18 10 2 59 51 43 35 27 19 11 3 60 52 44 36 63 55 47 39 31 23 15 7 62 54 46 38 30 22 14 6 61 53 45 37 29 21 13 5 28 20 12 4 bảng 2.3: bảng trật tự khóa pc-1 64 bít khóa ban đầu được chọn lấy 56 bít theo quy tắc đã nói ở trên, sau đó được đưa vào khối hoán vị pc-1
x	4	33 Bước 1: Khóa gốc sẽ được đi qua bảng hoán vị PC-1 Bảng PC-1 57 49 41 33 25 17 9 1 58 50 42 34 26 18 10 2 59 51 43 35 27 19 11 3 60 52 44 36 63 55 47 39 31 23 15 7 62 54 46 38 30 22 14 6 61 53 45 37 29 21 13 5 28 20 12 4 Bảng 3.6	40 8 48 16 56 24 64 32 39 7 47 15 55 23 63 31 38 6 46 14 54 22 62 30 37 5 45 13 53 21 61 29 36 4 44 12 52 20 60 28 35 3 43 11 51 19 59 27 34 2 42 10 50 18 58 26 33 1 41 9 49 17 57 25 bảng 2.2: bảng hoán vị ngược ip-1 lưu ý rằng hai hoán vị ip và ip-1 không có ý nghĩa gì về mặt mật mã mà chỉ tăng thêm tính phức tạp đồng thời nhằm tạo điều kiện cho việc “chip hóa” thuật toán des

Kết quả kiểm trùng với tài liệu: Tài liệu hệ thống - k20httt_pham_thi_thanh_thuy_luan_van_437.txt

Tỉ lệ sao chép: **0.413%**

Trang	Chỉ số	Tài liệu kiểm tra	Tài liệu gốc
x	5	75 Chọn hai số nguyên tố lớn p và q (ví dụ: p = 61, q = 53)	tạo hai số nguyên tố lớn p và q
76	6	Tính n = p * q và hàm Euler φ(n) = (p-1) * (q-1)	tính n = p × q và □(n) = (p-1).(q-1)

Kết quả kiểm trùng với tài liệu:
https://tailieu.vn/docview/tailieu/2013/20130128/nhutretho/tran_thi_kim_thuy_5862.pdf

Tỉ lệ sao chép: **0.207%**

Trang	Chỉ số	Tài liệu kiểm tra	Tài liệu gốc
x	7	Khởi tạo và phân bố khóa 3.3.1.1	□ quy trình giải mã gồm: khởi tạo, phân bố khóa và giải mã