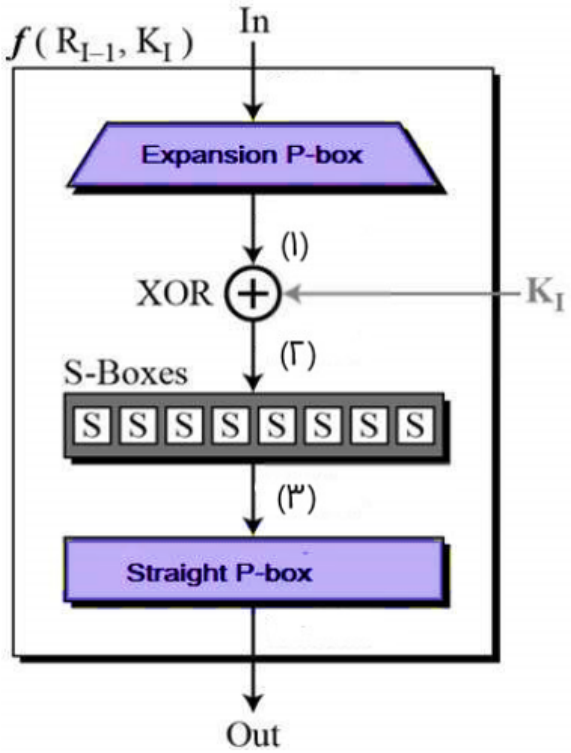
شروع	یکشنبه، 16 آبان 1400، 3:35 عصر
وضعیت	پایان‌یافته
پایان	یکشنبه، 16 آبان 1400، 3:39 عصر
زمان صرف شده	4 دقیقه 41 ثانیه
نمره	**8.75** از 10.00 (**88**٪)

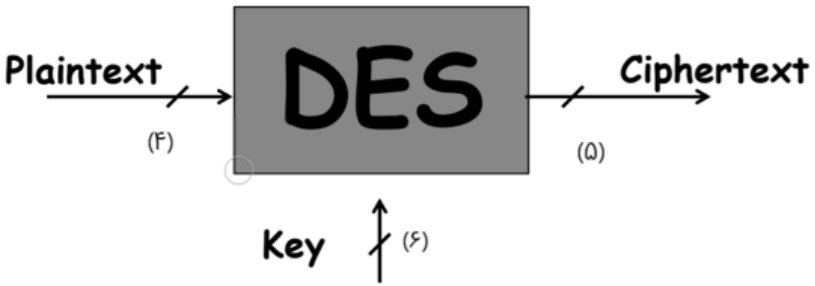
سؤال 1

درست

نمره 2.00 از 2.00

تصاویر زیر الگوریتم DES و تابع f آن را نشان می‌دهد، گزینه مناسب به جای اعداد در تصاویر به ترتیب از راست به چپ کدام است؟





- 48 بیت - 48 بیت - 48 بیت - 64 بیت - 64 بیت - 56بیت
- 32 بیت - 48 بیت - 48 بیت - 64 بیت - 64 بیت - 64 بیت

- 48 بیت - 48 بیت - 32 بیت - 64 بیت - 64 بیت - 56 بیت ✔
- 32 بیت - 48 بیت - 32 بیت - 64 بیت - 64 بیت - 56بیت

پاسخ شما صحیح می باشد

پاسخ درست «
48 بیت - 48 بیت - 32 بیت - 64 بیت - 64 بیت - 56 بیت » است.

سؤال 2

درست

نمره 2.00 از 2.00

در الگوریتم DES، مقدار ورودی به جعبه جایگشتی برابر ... بیت و مقدار ورودی به جعبه‌های جانشینی برابر ... بیت می‌باشد.

- 32 - 48
- 48 - 48
- 48 - 32 ✔
- 32 - 32

پاسخ شما صحیح می باشد

پاسخ درست «

32 - 48» است.

سؤال 3

درست

نمره 1.00 از 1.00

مطابق معیار شانون در طراحی یک سیستم رمزنگاری، هرچه کلید کوتاهی داشته باشیم امنیت و پیچیدگی محاسباتی کم‌تری خواهیم داشت.

یک گزینه را انتخاب کنید:

- صحیح
- غلط ✔

پاسخ درست گزینهٔ «غلط» است.

سؤال 4

پاسخ نیمه درست

نمره 3.75 از 5.00

کدام یک از موارد زیر در رابطه با Confusion و کدام در رابطه با Diffusion است؟

پنهان شدن رابطه بین متن رمز شده و متن اصلی با آن است.	Confusion	✗
این نوع از رمزنگاری تنها یک XoR ساده است.	Stream cipher	✓
پیچیده شدن رابطه متن رمز و کلید	Confusion	✓
پراکنده‌سازی ساختار آماری متن اصلی بر روی کل متن رمز شده	Diffusion	✓

پاسخ شما تا حدودی صحیح است

شما به درستی 3 گزینه را انتخاب کرده‌اید

پاسخ درست:

پنهان شدن رابطه بین متن رمز شده و متن اصلی با آن است. → Diffusion, این نوع از رمزنگاری تنها یک XoR ساده است. → Stream cipher,

پیچیده شدن رابطه متن رمز و کلید → Confusion,

پراکنده‌سازی ساختار آماری متن اصلی بر روی کل متن رمز شده → Diffusion