|  |  |  |
| --- | --- | --- |
|  | *به نام خدا*  **امنیت شبکه**  تمرینات سری اول | نیمسال دوم 95-94  مهلت تحویل: 10 اسفند |

1. مشخص كنيد هر يك از اعمال زير چه بعد يا ابعادي از امنيت (محرمانگي، تماميت، دسترس پذيري) را نقض مي­كنند.
   1. علي تمرين رضا را كپي مي كند.
   2. رضا سيستم احمد را از كار مي اندازد.
   3. علي مبلغ چك رضا را از 100000 ريال به 200000 ريال تغيير مي دهد.
   4. محمود امضاي علي را جعل مي كند.
   5. رضا آدرس IP سيستم محمود را براي دسترسي به كامپيوتر وي جعل مي كند.
2. محرمانگی و حریم خصوصی را تعریف کنید. تفاوت‏های آنها چیست؟ شرح ‏دهید.
3. چندین کلید ضعیف در الگوریتم رمزنگاری DES وجود دارد. یکی از آنها در ادامه آورده شده است.

00011111 00011111 00011111 00011111 00001110 00001110 00001110 00001110

* 1. سایر کلید‏های مشابه را بیابید.
  2. عیب استفاده از این کلید‏ها چیست؟ پاسخ خود را شرح دهید.

1. نشان دهید الگوریتم DES خاصیت متمم گیری دارد. برای این کار نشان دهید اگر C=Enc(K, P) آنگاه C’=Enc(K’, P’). (X’ متمم بیتی X است)
2. یکی از پیاده‏سازی‏های الگوریتم‏های رمز‏نگاری DES و AES را بیابید.
   1. برنامه کوچکی بنویسید که عمل رمز‏نگاری و رمزگشایی را توسط DES و AES انجام دهد.
   2. برنامه را طوری تغییر دهید که الگوریتم‏های فوق بتوانند در مد‏های کاری مختلف کار کنند.
   3. مد‏های ECB و CBC را مقایسه کنید.
   4. اثر بهمنی(Avalanche effect) را معرفی کنید.
   5. اثر بهمنی را در هر دو الگوریتم و در مد‏های ECB و CBC با هم مقایسه کنید.

|  |
| --- |
| **تذکرات** |
| * لطفا متن پاسخ خود را در قالب‏ یک فایل PDF، به همراه کد و سایر ملحقات به صورت یک فایل فشرده به آدرس [salaripanah.d+IUTNS@gmail.com](mailto:salaripanah.d+IUTNS@gmail.com) ارسال کنید. * نام فایل‌ها باید برابر با IUT-NS-studentNum باشد. * تمرینات باید به صورت انفرادی انجام شود. * به ازای هر روز تاخیر، 25 درصد از نمره تمرین کسر می‌شود و به تمرین با بیش از سه روز تاخیر، نمره تعلق نمی‌گیرد. |