تکلیف چهارم

مهدی حق‌وردی

۸ تیر ۱۴۰۳

فهرست مطالب

۱ دیفی–هلمن سه نفره

One possible protocol could be the following:

1. A, B, C each generate their private keys x_A, x_B, x_C
2. A, B, C each calculate $y_A = g^{x_A}$, $y_B = g^{x_B}$, $y_C = g^{x_C}$
3. A sends y_A to B, B sends y_B to C, C sends y_C to A.

4. A calculates $z_{CA} = y_C^{x_A}$, B calculates $z_{AB} = y_A^{x_B}$, C calculates $z_{BC} = y_B^{x_C}$.
5. A sends z_{CA} to B, B sends z_{AB} to C, C sends z_{BC} to A.
6. A calculates $k_{BCA} = z_{BC}^{x_A}$, B calculates $k_{CAB} = z_{CA}^{x_B}$, C calculates $k_{ABC} = z_{AB}^{x_C}$.

The above equality means that the three parties now know a common secret $k_{ABC} = k_{CAB} = k_{BCA}$

۲ رمزنگاری بهینه در برقراری یک نشست (session)

۳ معکوس ضربی

۴ در RSA

۱.۴ پیدا کردن d

۲.۴ پیدا کردن n، d و $\Phi(n)$

۳.۴ چرا e را عدد یک انتخاب نمی‌کنیم؟

۴.۴ حمله‌ی chosen-ciphertext روی RSA

۵.۴ آیا کلید regenrate شده امن است؟

۵ در Rabin

۱.۵ متن ۱۷ را رمز کنید

۲.۵ با استفاده از Chinese remainder theorem چهار متن آشکار احتمالی را پیدا کنید

۶ امنیت امضای دیجیتال RSA

۷ سوءاستفاده‌ی فرد مهاجم از روی ویژگی همریختی RSA

۸ سختی جعل در امضای الجمال