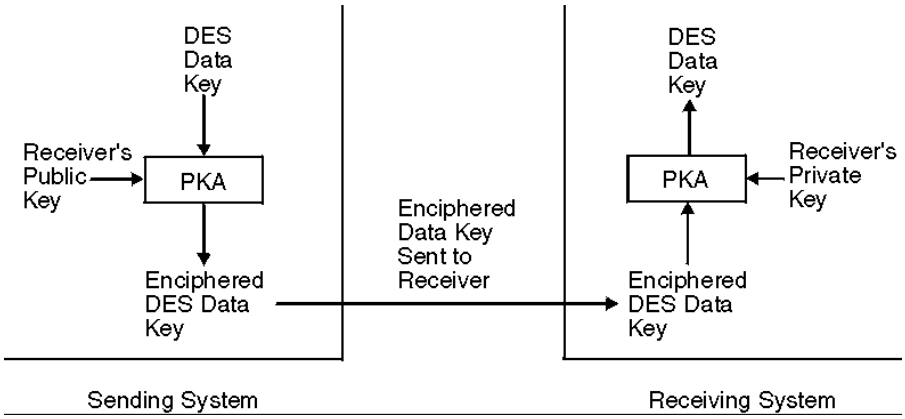
# HW3 – Keivan Ipchi Hagh - 9831083

## سوال اول)

کلید های مخفی میتوانند با استفاده از کلید های عمومی RSA بین سیستم ها با امنیت بالا منتقل بشوند، به گونه ای که سیستم های فرستنده و گیرنده نیاز به یک کلید مشترک برای تبادل کلید مخفی ندارند. در این حالت، فرستنده کلید مخفی را با استفاده از کلید عمومی گیرنده رمزنگاری کرده و به فرستنده ارسال میکند و سپس فرستنده کلید رمزنگاری شده را با استفاده از کلید مخفی خود بازگشایی میکند.

عکس زیر که از سایت IBM برداشته شده میتواند این انتقال را به خوبی به تصویر بکشد:




## سوال دوم)

برای الگوریتم های رمزنگاری مانند DES که دو طرفه هستند، رمزنگاری و رمزگشایی هر دو توسط یک الگوریتم یا یک کلید انجام میشود. به گونه ای که در رمزگشایی round key به طور برعکس حالت رمزنگاری استفاده میشود تا رمزگشایی صورت بگیرد. حال اگر از یک Hash Function به عنوان round key استفاده کنیم، عملا دیگر round key نخواهیم داشت و رمزنگاری و رمزگشایی با استفاده از یک الگوریتم انجام میشود.

در توضیح دقیق تر، از یک round key و بخشی از یک block استفاده میکند تا عمل رمزنگاری را با نصفه دیگر block انجام دهد. حال اگر به جای round key یک Hash Function استفاده کنیم، رمزنگاری دو طرفه خواهد شد.

## سوال سوم)

اول میدانیم $n = 35 = 5 * 7$ پس p و q برابر 7 و 5 خواهند بود که هر دو اعداد اول هستند. حال مقدار phi(n) طبق فرمول $phi(n)=(p-1)(q-1)$ برابر 24 خواهد شد. در گام بعد باید معادله $e * d = 1 \bmod 24$ را حل کنیم که در آن $e = 5$ است پس قطعا $d = 5$ خواهد شد تا معادله برقرار باشد.

# HW3 – Keivan Ipchi Hagh - 9831083

در قدم آخر 10^5 mod 35 برابر معادل 5 خواهد شد که پیام اصلی است.

## سوال چهارم)

الف) چون a = 9 پس طبق ( g^a mod p) و کلید خصوصی برابر 16 میشود.

ب) کلید خصوصی برابر 8 شده و کلید مشترک 3 میشود.

## سوال پنجم)

امضای دیجیتال خیلی به fingerprint شباهت دارد، به گونه ای که یک متن یا شیئ داریم و یک امضا، حال با ترکیب این دو توسط یک Hash Function آن را رمز کرده که با استفاده از PKI قابل تایید است. ویژگی های امضای دیجیتال:

- امنیت: با استفاده از ساختار PKI و ذخیره سازی کلید مخفی در جای امن، امنیت امضا های دیجیتال تضمین میشود.
- صرفه جویی هزینه: دیگر نیازی به قرارداد و کاغذ نیست و تمام فرایند در کامپیوتر انجام میشود.
- صرفه جویی زمانی: امضای دیجیتال هر زمانی میتواند انجام شود و محدودیت زمانی یا منابع نداریم چون فرایند سریعی است.

## سوال ششم)

به طور مختصر یک امضای کور آن است که امضا کننده تمام مفاد یا چیز هایی که امضا میکند را نمی بیند. دلیل اینکار حفظ امنیت قرار داد است زیرا برای مثال در دنیای کریپتو، نمیتوان همه اطلاعات را به کاربران نشان داد پس شما قرار دادی امضا میکنید که لزوما نمیدانید تمام محتویات داخل آن چیست.

از طرفی کلاهبرداران برای یافتن مفاد قرار داد و سود جویی از تکنیک های جدیدی استفاده میکنند تا آنها را بیابند که منجر به ساخته شدن روش های نوین کلاهبرداری میشود. مثال این موضوع درگاه پرداخت بانک است، زیرا که ممکن است صفحه نمایش هم شده باشد و عملا نمی توان مفاد قرار داد را بطور کافی داشت.

## سوال هفتم)

برای رمزنگاری: ابتدا N=p*q=143 میشود. سپس 3^11 mod 143 برابر 113 میشود که متن رمزنگاری ما است.

# HW3 – Keivan Ipchi Hagh - 9831083

برای رمزگشایی: phi(n)=(p-1)(q-1)=120 میشود. سپس باید معادله e * d = 1 mod 120 را حل کنیم که در آن e = 11 پس d = 11 میشود. برای محاسبه متن اصلی باید 113^11 mod 143 برابر 3 میشود که معادل متن اصلی است.