۱-کنترل دسترسی چیست

۲-حمله چیست

۳-امنیت اطلاعات چیست

۴-سیستم امنیت اطلاعات چیست

۵-رمزنگاری متقارن چیست

۶-محرمانگی و احراز هویت چیست

۷-الگوریتمdesچیست

۸-الگوریتم rsa چیست

۹-تصدیق پیام چیست

۱۰-سه مفهوم اساسی در امنیت اطلاعات را بیان کنید

پاسخنامه

۱-

اطمینان از دسترسی به دارایی‌ها به‌صورت مجاز و محدودشده بر اساس الزامات امنیتی و کسب‌وکار.

۲-

تلاش برای تخریب[۲]، افشا[۳]، تغییر[۴]، غیرفعال کردن، سرقت[۵] و دسترسی یا استفاده غیرمجاز[۶] از یک دارایی را حمله می‌نامند.

۳-

تلاش برای تخریب[۲]، افشا[۳]، تغییر[۴]، غیرفعال کردن، سرقت[۵] و دسترسی یا استفاده غیرمجاز[۶] از یک دارایی را حمله می‌نامند.

۴-

سیستم مدیریت امنیت اطلاعات یا ISMS، بخشی از سیستم کلان مدیریتی است که اساس آن بر رویکرد مخاطره کسب‌وکار بوده و شامل برقراری[۷]، پیاده‌سازی، عملیات، نظارت، بررسی، نگهداری و بهبود امنیت اطلاعات است.

۵-

رمزنگاری نامتقارن (Asymmetric) یا کلیدعمومی (Public Key)، نوعی رمزنگاری است که در آن، رمزگذاری و رمزگشایی با دو کلید متفاوت انجام می‌پذیرد. این دو کلید بانام‌های کلیدخصوصی (Private Key) و کلیدعمومی (Public Key) شناخته می‌شوند.

۶-

همان‌طور که گفته شد، درصورتی‌که فرستنده، پیام را با کلید خصوصی خود رمز نماید، فراهم‌کننده احراز هویت و درصورتی‌که پیام را با کلید عمومی گیرنده رمز نماید، فراهم آورنده محرمانگی است. اما درصورتی‌که پیام صرفاً با کلید خصوصی فرستنده رمز شده باشد، هر کاربری که کلید عمومی فرستنده را در اختیار داشته باشد، قادر به رمزگشایی پیام خواهد بود.

۷-

الگوریتم Data Encryption Standard(DES)، یک الگوریتم رمزنگاری متقارن است و در گروه رمزنگاری مدرن قرار می‌گیرد. الگوریتم DES عملیات رمزنگاری خود را به‌صورت بلوکی و بر اساس کلید محرمانه انجام می‌دهد.

۸-

الگوریتمRSA، یک الگوریتم رمزنگاری بلوکی نامتقارن (کلید عمومی) است. این الگوریتم از دو کلید با نام‌های کلیدخصوصی و کلیدعمومی، برای رمزگذاری و رمزگشایی استفاده می‌نماید. به دلیل خاصیت کلیدهای خصوصی و عمومی، این الگوریتم توانایی ارائه ویژگی‌هایی مثل احرازهویت و محرمانگی را نیز دارد. همچنین درصورتی‌که به همراه توابع درهم‌سازی مورد استفاده قرار گیرد، ویژگی‌هایی مثل امضای دیجیتال و سرویس عدم‌انکار را نیز فراهم می‌آورد.

۹-

توابع درهم‌سازی به‌تنهایی و همچنین در کنار الگوریتم‌های رمزنگاری متقارن می‌توانند امکان تصدیق پیام (Message Authentication) را فراهم آورند. با تصدیق پیام، گیرنده اطمینان حاصل می‌نماید که پیام دریافت شده دقیقاً همان چیزی است که ارسال‌شده؛ و در مسیر تبادل از خطراتی مثل تغییرات[۱]، حذف[۲]، درج[۳] و بازپخش[۴] مصون مانده است.

۱۰-

امنیت اطلاعات دارای سه مفهوم اصلی Confidentiality، Integrity و Availability است که به