مدرس: دکتر مجتبی رفیعی

نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

جلسه ۲ رمزنگاری

نگارنده: مرضیه آیت

۲۰ بهمن ۱۴۰۰

فهرست مطالب

۱ رمزنگاری (Cryptogrphy)

در این جلسه قرار است به بررسی دیدگاه دانشجویان نسبت به فضای امنیت پرداخته شود. در این راستا، موضوع را با طرح سول زیر ادامه میدهیم.

سوال: امنیت در محیط فیزیکی به چه معناست؟

۱ به عنوان مثال رأی‌گیری به صورت سنتی را در نظر بگیرید و آن را از حیث امنیتی تحلیل کنید.

۲ به عنوان مثال دیگر امنیت منزل خود را در نظر گرفته و تحلیل کنید.

با توجه به مطالب قبل، امنیت در محیط فیزیکی را به صورت زیر میتوان تعریف کرد:

"محافظت از هر آنچه برای ما ارزشمند است در مقابل تهدیدات عمدی و خصمانه یا غیر عمد (مثل بلای طبیعی، اشتباهات نا خواسته فردی) "

در مقابل محیط یا فضای فیزیکی، فضای مجازی یا فضای سایبری (Cyberspace) قرار داد. فضای مجازی یک مفهوم برای توصیف فناوری دیجیتال به هم پیوسته است.

اصل و اساس داراییها و ارزشهای ما در محیط سایبری را داده تشکیل میدهند. پس در ادامه روی امنیت داده متمرکز می‌شویم. سیستم رأی گیری الکترونیکی، ایمیل و موارد مشابه را در فضای سایبری در نظر گرفته و ویژگی‌های امنیتی در آنها را تحلیل و بررسی کنید.

برخی از این ویژگی‌ها در ادامه فهرست شده‌اند:

- حفظ محرمانگی،
- عدم دسترسی غیرمجاز،
- عدم تغییر غیرمجاز،
- عدم انکار،
- عدم جعل فرستنده یا صاحب داده،
- عدم افشا،
- دسترس پذیری،
- عدم مشاهده،

و بسیاری دیگر از موارد مشابه. لازم به ذکر است که ویژگیهای بالا ممکن است معادل یکدیگر از لحاظ مفهومی باشند و صرفا ذکر شدهاند که به مشابهت‌ها یا تفاوتهای جزئِی آنها دقت شود.
لازم به ذکر است که تعریف امنیت برای سامانه به پارامترهای مختلفی وابسته است که در ادامه به برخی از آنها اشاره شده است:

- نیازمندی‌های امنیتی سازمان متولی سامانه،
- سیاست‌ها و توافق‌های سازمان،
- موجودیت‌های حاضر در اکوسیستم سامانه مدنظر،
- تحمل پذیری سازمان در برابر هزینه‌های امنیتی.