① مفاهیم رمزنگاری

هسته اصلی رمزنگاری، ارتباط امن بین حداقل دو عامل به‌عنوان مثال آلیس و باب است. بر این معنی که هر فن ارتباط پیام‌هایی را رد و بدل می‌کنند که توسط دیگران قابل مشاهده است و هدف آن است که پیام طوری نوشته شود که به جز هر فن ارتباط، کسی از محتوای پیام تبادل شده داده‌ای که خاصیت اطلاع رهنگر داشته باشد، کسب نکند.

در این راستا آلیس و باب می‌بایست:

① آلیس و باب بر سر یک کلید محرمانه به توافق برسند.

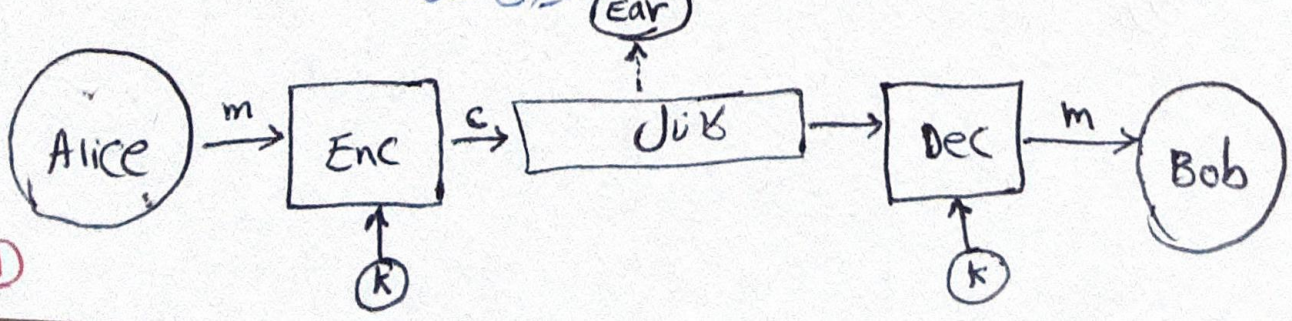
② با استفاده از کلید محرمانه و الگوریتم‌های تبدیل (رمزنگاری و رمزگشایی) اقدام به تبادل پیام کنند.

در دو ویژگی امنیتی پایه زیر را هم انتظار داریم که پوشش داده شود:

① محرمانگی (Confidentiality): غیر از دو سویه ارتباط که کلید محرمانه را در اختیار دارند، هیچ کس نتواند با دیدن پیام رمزی، اطلاعی از آن کسب نماید.

② صحت (Integrity): در صورتیکه پیام در بافتی توسط گیرنده دریافت راه تغییر پیدا کرده باشد، گیرنده متوجه آن می‌شود.

شکل زیر سناریو حل مسئله ارتباط امن را به تصویر می‌کشد.



در ادامه اصطلاحات (استاندارد) موجود در مسائل ارتباط امن فهرست شده‌اند:

- متن آشکار (Plaintext): پیام اصلی (رمز نشده) اطلاق می‌شود.
- متن رمز (ciphertext): به پیام رمز شده اطلاق می‌شود.
- رمزگذاری (Encipher یا Encryption): به الگوریتم تبدیل متن آشکار به متن رمز اطلاق می‌شود.
- رمزگشایی (Decipher یا Decryption): به الگوریتم استخراج متن آشکار از متن رمز اطلاق می‌شود.

در رابطه با علم رمزنگاری نیز تعاریف اولیه زیر ارایه شده است.

- رمزنویسی (یا رمزنگاری) (cryptography): به علم اصول و روش‌های رمزگذاری اطلاق می‌شود.
- تحلیل رمز (cryptanalysis): به علم اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید اطلاق می‌شود.
- رمزشناسی (cryptology): به علم حاصل از ترکیب رمزنویسی و تحلیل رمز اطلاق می‌شود.

(۲) رمزنگاری متقارن

رمزنگاری کلید-متقارن (Symmetric-key Encryption) یا به اختصار رمزنگاری متقارن تنها نوع رمزنگاری تا قبل از ۱۹۷۶ میلادی است. این نوع رمزنگاری به نام‌های رمزنگاری کلید مخفی و رمزنگاری تک کلیدی نیز معروف است.

علت استفاده از واژه متقارن در این نوع رمزنگاری آن است که هر دو طرف ارتباط (فرستنده و گیرنده) از یک کلید مشترک برای تبدیلات مورد نیاز استفاده می‌کنند. لازم به ذکر است که تمامی رمزنگاری‌های کلاسیکی که در ادامه معرفی می‌شوند جزء این دسته به حساب می‌آیند.

(۳) اصل کرشهف: اصل کرشهف در واقع دو فرض را برای صریستم رمزنگاری الزامی می‌داند:

۱- الگوریتم‌های رمزنگاری (رمزگشایی، رمزگذاری و تولید کلید) می‌بایست آشکار باشد.

۲- امنیت یک سیستم رمزنگاری بر اساس مخفی بودن کلید تعریف می‌شود.

(۴) ابعاد رمزنگاری: سیستم‌های رمزنگاری را می‌توان بر اساس پارامترهای مختلفی رده‌بندی کرد. در ادامه برخی از مهم‌ترین این پارامترها و دسته‌بندی‌ها آورده شده است.

۱ تبدیلات مورد استفاده برای رمزگذاری:

- جانشینی (substitution): هر عنصر متن آشکار با عنصر دیگری (از الفبا) موجود در متن آشکار ۳ جایگزین می‌شود.

- جابجایی (Transposition): متن رمز از جابجایی عناصر متن آشکار بدست می آید.

۲ تعداد کلیدهای مورد استفاده برای رمزنگاری:

- یک کلید حفره ای مشترک: که معرف سیستم های رمزنگاری متقارن هستند.
- یک جفت کلید برای هر طرف ارتباط: که معرف سیستم های رمزنگاری نامتقارن هستند که هر طرف ارتباط در آن یک کلید عمومی و یک کلید حفره ای مربوط به خود دارد.

۳ روش پردازش متن آشکار و تولید متن رمز:

- بلوکی: متن آشکار بلوک بندی شده و سپس هر بلوک تبدیل به متن رمزی می شود.
- جریانی: عناصر متن آشکار به طور پیوسته به ورودی داده می شود و در هر لحظه یک عنصر رمز شده خارج می شود.

۵ عملات و تحلیل رمزنگاری

در حالت کلی هدف از حمله به یک سیستم رمزنگاری را می توان در موارد زیر خلاصه کرد:

۱ استخراج کلید

۲ استخراج متن آشکار از متن رمز شده

با این حال اهدافی همچون استخراج یک تابعی از متن آشکار یا حتی یک بیت از اطلاعات نیز می تواند هدف حمله را تعریف کند.

نحوه حمله به یک سیستم رمزنگاری می‌تواند براساس پارامترهای زیر باشد:

۱. بررسی خصوصیات الگوریتم‌های رمزنگاری،

۲. بررسی مجموعه‌ای از متن‌های آشکار و رمز شده که به طرق مختلف ممکن است در دسترس مهاجم قرار گیرد.

(۴) براساس اطلاعاتی که مهاجم (تحلیل‌گر) یک سیستم رمزنگاری در اختیار دارد، می‌توان انواع حملات زیر را تعریف کرد:

۱. حمله متن رمزی تنها (ciphertext only attack): در این حمله، مهاجم از الگوریتم‌های رمزنگاری و تنها متن رمزی آگاه است.

تعدادی

۲. حمله متن آشکار شناخته شده (known Plaintext attack): در این حمله، مهاجم علاوه بر الگوریتم‌های رمزنگاری و متن رمزی، یک یا چند جفت متن آشکار و رمز شده معادل آن را هم می‌داند.

۳. حمله متن آشکار انتخابی (chosen Plaintext attack): در این حمله، مهاجم علاوه بر الگوریتم‌های رمزنگاری و متن رمزی، یک یا چند جفت متن آشکار و رمز شده معادل آن را هم می‌داند به نحوی که متن آشکار زوج‌های مذکور را خود انتخاب می‌کند.

۴. حمله متن رمز انتخابی (chosen ciphertext attack): در این حمله، مهاجم علاوه بر الگوریتم‌های رمزنگاری و متن رمزی، یک یا چند جفت متن آشکار و رمز شده معادل آن را هم می‌داند به نحوی که متن رمزی زوج‌های مذکور را خود انتخاب می‌کند.

۵ حمله متن انتخابی (chosen text attack): در این حمله، مهاجم علاوه بر متن رمز شده، الگوریتم های رمزنگاری و متن رمزی، یک یا چند جفت متن آشکار و معادل رمز شده آنها را هم می داند به نحوی که متن رمزی یا متن آشکار زوج های مذکور را خود انتخاب می کند.

۶ مهاجم براساس میزان دانشی که در اختیار دارد و همچنین قدرت محاسباتی خود، استراتژی های حمله متفاوتی را ممکن است در برابر یک سیستم رمزنگاری را در نظر بگیرد. یکی از ابتدایی ترین استراتژی ها حسبت وجوی تمام حالات (Brute force search) است. در این استراتژی حمله فرض بر آن است که متن آشکار قابل شناسایی است.

شکل زیر استراتژی حسبت وجو تمام حالات را که به عنوان یک استراتژی همواره (اما زمانبر) شناخته می شود را برای برخی از سیستم های رمزنگاری از حیث زمانی نشان می دهد.

سیستم رمزنگاری	اندازه کلید (بیت)	اندازه فضای کلید	ماشین با امکانات و توانایی برای یک رمزگشایی	ماشین با امکانات و توانایی برای 10^6 رمزگشایی
DES	۵۶	$2^{56} = 7.2 \times 10^{16}$	2^{55} MS = ۱۴۲ سال	۱۰۱۰ ساعت
AES	۱۲۸	$2^{128} = 3.4 \times 10^{38}$	2^{127} MS = 5.4×10^{24} سال	5.4×10^{18} سال
3DES	۱۶۸	$2^{168} = 37 \times 10^{50}$	2^{167} MS = 5.9×10^{36} سال	5.9×10^{30} سال
substitution code	۲۶ کاراکتر	$26! = 4 \times 10^{26}$	4×10^{27} MS = 6.4×10^{12} سال	6.4×10^{6} سال

نکته: در جدول بالا، دو ستون آخر (سمت چپ) بیانگر زمان مورد نیاز برای حمله موفق با استراتژی مذکور است.