به نام خدا

دانشکده‌ی علوم ریاضی

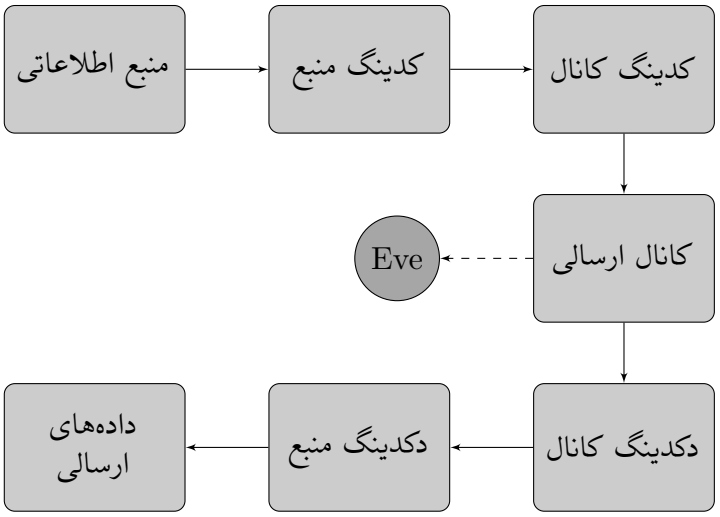
مقدمه‌ای بر رمزنگاری ۱۵ بهمن ۱۳۹۱

جلسه‌ی ۱ : مقدمه

مدرس: دکتر شهرام خزائی *نگارنده: سهی صالحیان قمصری*

۱ مفاهیم اولیه

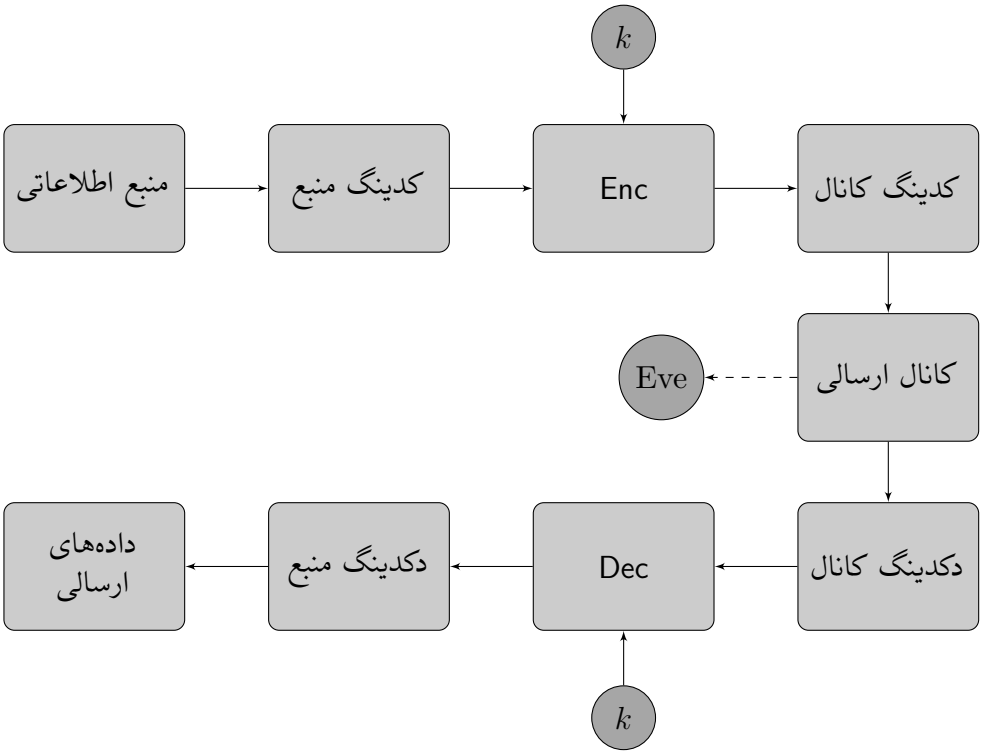
امروزه در رمزنگاری[۱] مسائل گوناگونی مانند پروتکل‌های رمزنگاری[۲] مطرح می‌باشد ولیکن موضوع اصلی این درس اولیه‌های رمزنگاری[۳] و درک اهمیت آن‌هاست.
تاکید بر این نکته که رمزنگاری و کدینگ[۴] دو امر متفاوت می‌باشند، امری الزامی‌ست. در واقع کدینگ قسمتی از عملیات انتقال یک پیام است. دو نوع کدینگ وجود دارد. نوع اول، کدینگ منبع است که جزئی از مدل اولیه زیر است که انتقال اطلاعات را نشان می‌دهد.



در شکل بالا، منبع اطلاعاتی می‌تواند شامل هر نوعی از اطلاعات از قبیل: صوت، تصویر، متن و ... باشد. وظیفه «کدینگ منبع» نیز فشرده‌سازی اطلاعات موجود در منبع و تبدیل کردن‌شان به بیت‌های ۰ و ۱ است.

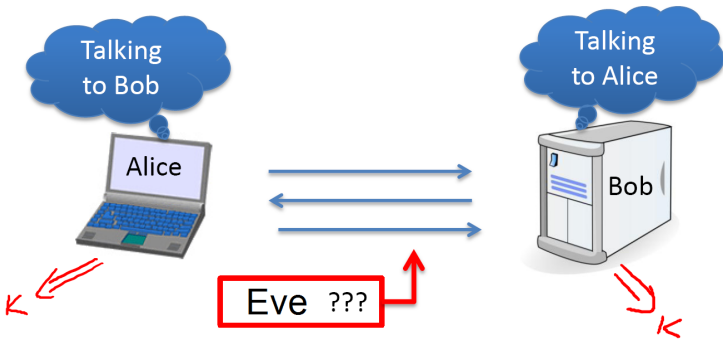
[۱] cryptography
[۲] cryptographic perimitives
[۳] cryptographic protocoles
[۴] coding

برای کاهش احتمال خطای کانال نیاز به اضافه کردن نوع دوم از کدینگ، یعنی «کدینگ کانال»، میان «کدینگ منبع» و «کانال ارسالی» است. Eve یا حمله کننده[۵] و یا مهاجم[۶] کامپیوتری است که قصد حمله و دزدیدن اطلاعات را دارد و همان طور که در شکل نشان داده شده است هدف حمله‌هایش کانال ارتباطی است. در واقع یکی از اهداف رمز نگاری محرمانگی[۷] و جلوگیری از چنین حملاتی است. در رمزنگاری برای رسیدن به هدف «محرمانگی» الگوریتم‌های Enc و Dec را به دیاگرام بالا اضافه می‌کنیم که هر دو به کلید رمز k وابسته‌اند:



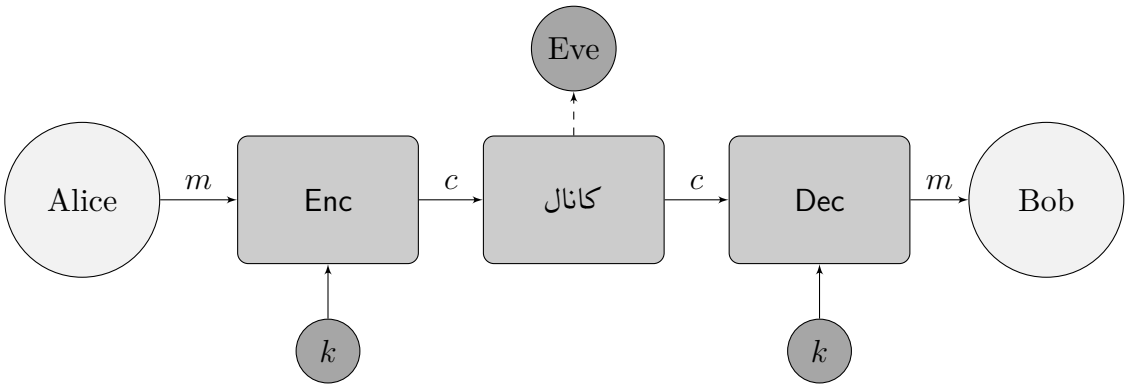
در واقع تنها قسمتی از دیاگرام بالا که مربوط به الگوریتم‌های رمزنگاری است، مد نظر ما در این درس می‌باشد. سه قسمت «کدینگ کانال»، «کانال» و «دکدینگ کانال» را مجموعاً «کانال» می‌نامیم. فرض می‌کنیم کانال‌ها بدون خطا بوده و از بررسی‌اشان صرف نظر می‌کنیم.
حال دو کامپیوتر Alice و Bob را در نظر بگیرید که از طریق کانالی که توسط Eve رصد می‌شود، قصد مکالمه دارند:

[۵] attacker
[۶] adversary
[۷] confidenciality



شکل ۱: Alice و Bob قصد مکالمه دارند.

حال فرض کنید Alice قصد ارسال متن اصلی[۸] m را به Bob از طریق این کانال دارد. (توجه کنید که بخش‌های کدینگ و دکدینگ منبع مورد توجه ما نیستند و m را به صورت رشته‌ای از حروف روی یک الفبا مانند الفبای $\{۰, ۱\}$ در نظر می‌گیریم). ابتدا با استفاده از الگوریتم رمزنگاری Enc عملیات رمزکردن[۹] متن m و تبدیل آن به متن رمزی[۱۰] c انجام می‌شود. پس از ارسال متن رمزی c از طریق کانال و دریافت آن در سمت دیگر، نوبت به رمزگشایی[۱۱] می‌رسد. این کار توسط الگوریتم رمزگشایی Dec انجام می‌شود و پس از آن متن اصلی m در اختیار Bob قرار می‌گیرد. هر دو الگوریتم Enc و Dec نیازمند کلید مشترک k هستند (معمولاً ۸۰ الی ۲۵۶ بیت) که باید آن را از طریق کانال امنی که Eve به آن دسترسی ندارد، به اشتراک بگذارند.[۱۲] دیاگرام ذیل، عملیات بالا را نشان می‌دهد:



حال به شرح نمونه ساده‌ای از یک سیستم رمز می‌پردازیم.

۲ سیستم رمز سزار

متن رمزشده زیر توسط Eve رصد شده است:

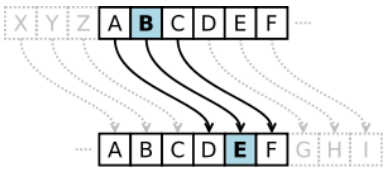
[۸] plaintext
[۹] encryption
[۱۰] ciphertext
[۱۱] decryption
[۱۲] key establishment

"L dp d fubswrjudskhu dqg L pdnh vhfuhw frghv"

آیا می‌توانید حدس بزنید که متن اصلی چه بوده است؟
در واقع با کمی بررسی کلمات تک و دو حرفی زبان انگلیسی درخواهید یافت که در متن رمزشده هر یک از حروف زبان انگلیسی به سه حرف بعد از خود شیفت[۱۳] داده شده‌اند. با جایگزینی هر حرف رمزشده با حرف اصلی‌اش، متن

"I am a cryptographer and I make secret codes"

حاصل خواهد شد.
به طور مثال تک حرف "L" که دو مرتبه در متن رمزشده مشاهده می‌شود و همچنین تک حرف "d" یا جایگزین کلمه تک حرفی "a" و یا "I" می‌باشند ... .
این سیستم رمز، سیستمی است که ژولیوس سزار[۱۴] در حوالی سال ۵۰BC از آن استفاده می‌کرده است و به رمز سزار[۱۵] معروف است.



شکل ۲: سیستم رمز سزار

برای تعمیم این سیستم رمز می‌توان به جای شیفت سه تایی از شیفت kتایی حروف استفاده کرد. بدین معنا که برای رمز کردن متن اصلی، هر حرف را به k حرف بعد از آن شیفت دهیم که در این‌صورت اندازه فضای کلید[۱۶] (که با $\mathcal{K}$ نشان داده می‌شود) برابر با تعداد حروف انگلیسی یعنی ۲۶ خواهد بود، یعنی $|\mathcal{K}| = ۲۶$.
در اصلی به نام اصل کیرشهف[۱۷] ، فرض را بر عمومی بودن الگوریتم‌های رمزنگاری قرار خواهیم داد و در این‌صورت تمام امنیت به عهده «کلید» قرار خواهد گرفت. بنابراین هر یک از ماشین‌های Enc و Dec در اختیار هر یک از Alice، Bob و Eve قرار دارد؛ اما کلید k میان Alice و Bob محرمانه است و Eve به آن دسترسی ندارد.
برای سیستم رمز سزار داریم:

$$\mathsf{Enc}_k(m_۱ m_۲ \dots m_n) = c_۱ c_۲ \dots c_n$$

که برای محاسبه هر c_i رابطه زیر برقرار است:

$$c_i = m_i + k \mod ۲۶$$

و این بدان معناست که برای شکستن رمز سزار کافی‌ست ۲۶ کلید (تعداد حروف زبان انگلیسی) را بررسی کنیم و k را بیابیم؛ در نتیجه فضای کلید ۲۶ عضوی، کوچک و قابل جستجوست.
الگوریتم‌های رمزنگاری و رمزگشایی که در عمل مورد استفاده قرار می گیرند، الگوریتم‌هایی بسیار سریع هستند. در حال حاضر، یک کامپیوتر معمولی برای چنین الگوریتم‌هایی به راحتی فضاهای کلید با اندازه‌های حداکثر حدود

[۱۳] shift
[۱۴] Julius Caesar
[۱۵] Caesar cipher
[۱۶] key space
[۱۷] Kerckhoffs???

$۲^{۵۰}$ را در زمان قابل تحملی جستجو می‌کنند. بدین صورت که با فرض عمومی بودن الگوریتم‌های Enc و Dec همه کلیدهای ممکن را بررسی کرده و کلید موردنظر را می‌یابند. البته هزینه جستجوی تمام فضای کلیدی با اندازه $۲^{۸۰}$ در حال حاضر زیاد است و این اندازه، فضای کلید مناسبی برای سیستم‌های رمز در کاربردهایی که حساسیت زیادی نمی‌طلبند، خواهد بود. در واقع برای سطوح بالاتر امنیت می‌توان از کلیدهای ۱۲۸ - ۲۵۶ بیتی استفاده نمود.
چگونه فضای کلید را در رمز سزار بیشتر کنیم؟
یک پاسخ می‌تواند بدین‌صورت باشد که m را به صورت ذیل به c بنگاریم:

$$c = am + b \mod ۲۶$$

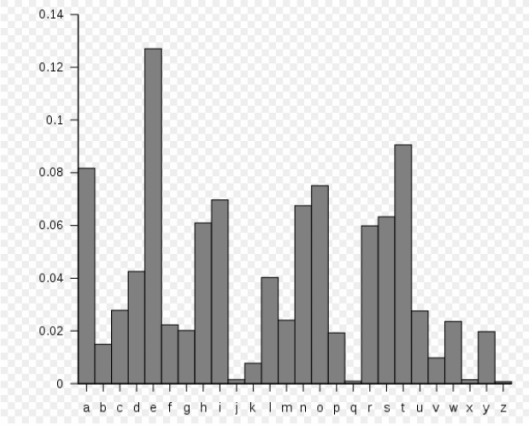
که کلید k به صورت $k = (a, b)$ تعریف می‌شود که:

$$\gcd(a, ۲۶) = ۱$$

برای محاسبه اندازه فضای کلید خواهیم داشت:

$$|\mathcal{K}| = \varphi(۲۶) \times ۲۶ = ۱۲ \times ۲۶$$

آیا باز هم می‌توان رمز سزار را تعمیم داد؟
بله! هر جدول دلخواهی را می‌توان درنظر گرفت که حروف زبان انگلیسی را به یک جایگشت دلخواه از آن می‌برد و این جدول همان کلید رمز خواهد بود. در نتیجه اندازه فضای کلید حداکثر $|\mathcal{K}| = ۲۶! \approx ۲^{۸۸}$ می‌باشد. به نظر می‌رسد که این مقدار به اندازه کافی بزرگ باشد که جستجوی کلید در آن به راحتی انجام‌پذیر نباشد؛ ولیکن در این‌جا مسئله دیگری به نام افزونگی[۱۸] مطرح می‌شود. در واقع حروف زبان انگلیسی دارای فرکانس حضور خاص خود در یک متن می‌باشند. مثلاً بیشترین فرکانس‌های حضور متعلق به حروف E، T و A است.
در واقع با استخراج فرکانس حروف در متن رمزشده و انطباق آن با جداول موجود در صورتی که طول متن به اندازه کافی بزرگ باشد، می‌توان جدول کلید به کار برده شده را یافت؛ در نتیجه به طور کلی می‌توان بیان کرد که به علت فرکانس حروف زبان انگلیسی، رمز سزار، رمز مناسبی نیست. در ذیل جدول کاملی از فرکانس حروف زبان انگلیسی را مشاهده می‌کنید:



[۱۸] redundancy

E	12.7%	M	2.4%
␣	12.0%	W	2.4%
T	9.8%	F	2.2%
A	8.2%	G	2.0%
O	7.5%	X	2.0%
I	7.0%	P	1.9%
N	6.7%	B	1.8%
S	6.3%	V	1.0%
H	6.1%	K	0.8%
R	6.0%	J	0.1%
D	4.2%	Q	0.1%
L	4.0%	Y	0.1%
C	2.8%	Z	0.1%
U	2.8%		

جدول ۱: فرکانس حضور حروف در زبان انگلیسی با در نظر گرفتن حرف فاصله

۳ اهداف رمزنگاری

اهداف رمزنگاری را تحت سه هدف کلی زیر می‌توان تقسیم‌بندی کرد:

۱. محرمانگی[۱۹]

۲. صحت و جامعیت[۲۰]

۳. احراز هویت[۲۱]

رمزنگاری برای دستیابی به هدف محرمانگی مورد استفاده قرار می‌گیرد. برای اطمینان از صحت و دست‌نخوردگی پیام رمزشده ارسالی از ابزارهای دیگری مانند امضای دیجیتال[۲۲] و MAC[۲۳] استفاده می‌شود که در این درس به طور مفصل با آن‌ها آشنا خواهیم شد.
ابزارهایی که سه هدف فوق را برآورده می‌کنند، ابزارهای پایه در رمزنگاری هستند که از آن‌ها برای ساخت پروتکل‌های پیچیده‌ای مانند پول دیجیتالی[۲۴] و رأی‌گیری الکترونیکی[۲۵] استفاده می‌شود که اهداف امنیتی دیگری مانند گمنامی[۲۶] را فراهم می‌کنند.

[۱۹] confidenciality
[۲۰] integrity
[۲۱] authentication
[۲۲] digital signature
[۲۳] message authentication code
[۲۴] digital cash
[۲۵] electronic voting
[۲۶] anonymity