رمزنگاری

رمزنگاری (Cryptography) از دو واژه **رمز** (Crypt) و **نگارش** (Graphy) پدید آمده است. هدف این علم بررسی و مطالعه اطلاعات رمزی و مخفیست. علم رمزنگاری به دو دسته مهم کلاسیک و مدرن تقسیم می‌گردد. تعریف رمزنگاری مدرن کمی با رمزنگاری کلاسیک که در بالا ارائه شد متفاوت است. امروزه رمزنگاری یکی از شاخه‌های ریاضی و علوم کامپیوتر دانسته می‌شود. همچنین این علم رابطه تنگاتنگی با علوم *نظریه اطلاعات* ، *امنیت رایانه‌ای* و مهندسی داراست.

در دنیای امروز، با رشد اینترنت و امکانات ارتباطی دیگر، نقش امنیت و تضمین صحت روابط بیشتر و بیشتر می‌گردد. پیچیدگی‌های روابط انسانی مانند اعتماد متقابل در روابط الکترونیکی وجود ندارند، از این رو بایستی یک علم شرایط را آماده و این روابط را تضمین نماید. با این تعریف، رمزنگاری علم تضمین ارتباطات است، بطوری که بدون رمزنگاری، هیچ تضمینی در دنیای ارتباطات دیجیتال وجود ندارد.

رمزنگاری کلاسیک به طور کلی به **رمزگذاری** (Encryption) محدود می‌شود که البته قسمت بسیار مهمی از رمزنگاری مدرن را نیز به خود اختصاص می‌دهد. رمزگذاری روند تبدیل اطلاعات عادی به اطلاعات غیرقابل کشف و تمیز و رمزگشایی (Decryption) معکوس این روند تعریف می‌شوند. واضح است که رمزگذاری از گذشته‌های بسیار دور، اهمیت داشته است زیرا همواره رمز باقی ماندن اطلاعات نقش مهمی در زندگی بشر ایفا کرده است.

رمزنگاری مدرن علاوه بر رمزگذاری، شاخه‌های مهم دیگری را نیز در بر می‌گیرد از جمله **رمزنگاری نامتقارن ، توابع فشرده ساز، احراز هویت پیام و افراد، اعداد تصادفی، امضاهای دیجیتال و ...**

علم رمزنگاری علاوه بر جذابیت و ویژگی‌های منحصر بفرد خود که آنها را از هویت رمزگونه خویش که با ریاضیات نیز در تعامل است بدست آورده، پیچیدگی بسیار زیادی نیز داراست؛ تا حدی که بسیاری از بزرگان ریاضی و رمزنگاری روز این علم را دشوارترین علوم دانسته‌اند. برای تسلط کافی به مباحث رمزنگاری از جمله *آنتروپی اطلاعات*، تلاش بسیار کافی نیست بلکه فرد باید تفکر رمزنگاری داشته باشد. از دشوارترین مباحث رمزنگاری که همیشه طرفداران بسیاری را به این علم گرایش داده، **رمزشکنی** (Cryptanalysis) را می‌توان نام برد. رمزشکنی فرایند شکستن تمامی تلاش به کار رفته یا قسمتی از آن برای رمزگونه سازی اطلاعات تعریف می‌شود.

امروزه رمزنگاری با جذب پرتلاشترین دانشمندان و نوابغ جهان، با رشدی باور نکردنی روند رسیدن به پرکاربردترین علوم را طی می‌کند.

Syllabus

- موارد مهم کاربرد رمزنگاری (بدون جزئیات)
- رمزنگاری کلاسیک
  - رمزنگار Caesar
    - تعریف رمزنگار و خواص آن
    - اصطلاحات رمزنگاری
    - مدل‌سازی ریاضی و معیارهای سنجش یک رمزنگار
    - حملات مرسوم و حملات ویژه سزار (Frequency Analysis)
  - رمزنگار Affine
    - روند بررسی یک رمزنگار
    - مزایا و معایب نسبت به سزار
    - نتیجه گیری
  - سیر تکاملی رمزنگارهای کلاسیک و رمزهایدارای ویژگی‌های بارز
    - رمزهای ابتدایی مانند Pigpen, Nihilist, Skytale
    - رمزهای Transposition
      - تعریف Substitution و Permutation
      - رمزهای Rail Fence, Route, Columnar, Double, Myskowski, Disrupted
      - تعریف آنتروپی اطلاعات
    - رمزهای مربعی
      - تعریف Fractionation
      - رمز Alberti
      - رمزهای Two-Square, Four Square
      - رمزهای Polybius, Playfair

§ رمزهای پخش کننده و ماتریسی

- رمز Hill
- تعریف Diffusion , Confusion

§ رمزهای جدولی و چندحرفی

- رمز معروف ویگنر (Vigenere)
- متدهای شکستن ویگنر (Kasiski و IoC)
- رمزهای Autokey

- از رمزنگاری کلاسیک به رمزگذاری مدرن

§ کلاد شانون و معجزه One-Time Pad

§ دستگاه Enigma

§ رمزها و دستگاه‌های رمزنگاری در جنگ جهانی دوم و تاثیرات آنها

§ رمزگذاری عملی و مولد اعداد تصادفی

- مولد LCG و ضعف آن، مولد Mersenne Twister, LFG و ...

§ رمزهای جریانی (Stream Cipher)

- رمزنگاری مدرن

o رمزنگاری متقارن

§ Lucifer و رمزنگاران در ابهام و سردرگمی

§ DES، استانداردی قابل اطمینان

§ رقابت AES و کمال رمزگذاری با برنده شدن Rijndael

§ تکامل نهایی و حملات Linear و Differential

o رمزنگاری نامتقارن

§ لزوم رمزنگاری نامتقارن

§ مدل‌سازی و تعاریف ریاضی (قفل دو کلیده)

- رمز رابین و الگوریتم اشتراک کلید Diffie-Hellman
- RSA و فتح رمزنگاری نامتقارن
    - پیاده‌سازی و موانع
    - حملات مرسوم
    - نقاط ضعف
- لگاریتم گسسته و ElGemal
    - حملات و نقاط ضعف
- میدان‌های محدود جمعی و خم‌های بیضوی، تحولی عظیم
- پیاده‌سازی و مشکلات امروزه رمزنگاری نامتقارن (سرعت، دقت)

o توابع چکیده‌ساز

- CRC-32 و تضمین صحت پیام
- MD5 و تضمین امنیت پیام
    - نقاط ضعف و سردرگمی
    - شکسته شدن ناباورانه MD5
- SHA-1 و امضاهای دیجیتالی مبتنی بر چکیده‌پیام
- حمله روز تولد و SHA-2

o امضاهای دیجیتال و کدهای اهراز هویت پیام و فرستنده

- امضای دیجیتال مبتنی بر رمزنگاری نامتقارن
- امضای دیجیتال مبتنی بر کدهای اهراز هویت
- امضای دیجیتال مبتنی بر چکیده
- امضای دیجیتال مستقل
    - استاندارد DSS