



# فصل اول: مقدمات درس

در این فصل مروری مختصر بر مفاهیم پایه‌ای امنیت در شبکه‌ها خواهیم داشت.

امنیت سیستم‌های کامپیوتری

ابوالفضل دیانت

آخرین ویرایش: ۱۲ خرداد ۱۴۰۰ در ساعت ۲۳ و ۴۹ دقیقه

## فهرست مطالب

۱	در مورد این درس ...
۷	رمزنگاری تا قبل از شانون
۱۱	مراجع
۱۴	فهرست اختصارات
۱۵	واژه نامه انگلیسی به فارسی
۱۶	واژه نامه فارسی به انگلیسی

در مورد این درس ...

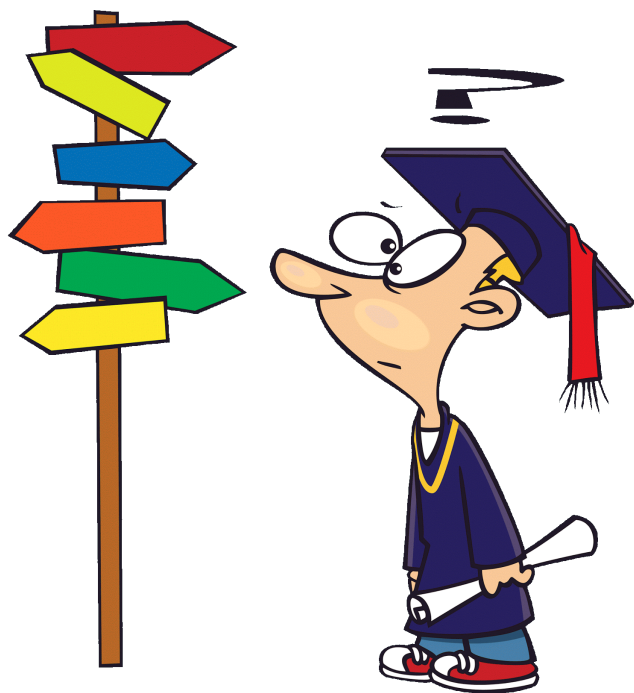
از گذشته‌های دور امنیت جایگاه مهمی در زندگانی ما ایفا می کرد اما فکر می کردیم امنیت تنها یعنی محرمانه ماندن پیام.

رمز دوران بچگی ما:  $\oplus \searrow \searrow \oslash \circledast \oplus \searrow \odot \boxplus \boxtimes$

هر ۳۹ ثانیه یک حمله توسط هکرها رخ می دهد. پیش بینی می شود که ۶ تریلیون دلار به صورت جهانی صرف امنیت سایبری شود.

چرا امنیت هنوز زنده است ....

چرا باید امنیت بدانیم؟؟؟



♠ فصل اول: مفاهیم و واژه‌های کلیدی در بحث امنیت شبکه

♠ فصل دوم: ریاضیات رمز و رمزنگاری نامتقارن

♠ فصل سوم: رمزنگاری متقارن الگوریتم‌های DES و AES

♠ فصل چهارم: امنیت در شبکه‌های کامپیوتری



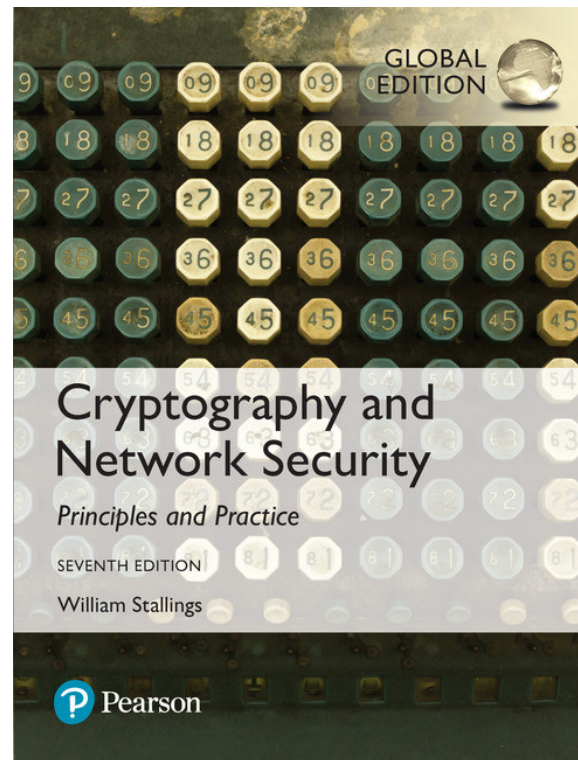
- امتحان‌های کوتاه کلاسی (هفت یا هشت نمره)
- تمرین‌ها (سه نمره)
- پروژه‌ها (چهار نمره)
- یادداشت کلاسی (دو نمره)
- امتحان پایان ترم (سه یا چهار نمره)
- فعالیت کلاسی (0.25 نمره)





نکته

مجموع از بیست نمره


[1] William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education Limited, 2017.



تمرین‌ها، کوییزها و اطلاع‌رسانی‌ها به صورت متمرکز در [lms.iust.ac.ir](https://lms.iust.ac.ir) صورت می‌پذیرد. 

تعیین نماینده برای کلاس 

امتحان‌های کوتاه هر هفته روزهای یک‌شنبه 

عضویت در کانال تلگرامی درس (لینک در LMS درس) 

تمرین‌ها به صورت تایپ‌شده و با  $\text{LATEX}$  باید تحویل داده شود (20 + 80). 

کلاس‌های اندروید برای آماده‌سازی برای پروژه خواهید داشت. 

لطفاً کپی نکنید!!! 



،مزننگاری تا قبل از شاننون

# تاریخچه رمزنگاری (Cryptography)

نخستین مفهوم در امنیت: رمزنگاری (Cryptography) 📖

قدمتی هزاران ساله از هیروگلیف‌ها گرفته تا Atabash و رمزنگاری آرشیلوس. 📖

نخستین الگوی مدون سامانه‌های رمزنگاری: الگوریتم سزار (Ceasar) 📖

This is an example → Wklv lv dq hadpsoh.



رمزنگاری (Cryptography) که برگرفته از دو کلمه یونانی krypto به معنای محرمانه و graphien به معنای نوشتن است، به جرات می‌توان گفت قدمتی هزاران ساله دارد؛ گرچه باید گفت که عمر نگاه علمی به این موضوع، از صد سال تجاوز نمی‌کند. هیروگلیف‌های حک‌شده بر روی سنگ‌ها (حروفی که با کشیدن تصویرهایی از جانوران و اشیاء پدید آمده باشد - Hieroglyph)، در ۱۹۰۰ سال پیش از میلاد مسیح در تمدن باستانی مصر، شاید نخستین تلاش بشر در مسیر علم رمزنگاری بود، گرچه به نظر می‌رسد هدف مصریان باستان از این کار مخفی کردن پیام نبوده، بلکه برعکس افزایش جذابیت کتیبه‌ها بوده است. اولین نمونه از این نوع کدگذاری را در آرامگاه مربوط به یکی از اشراف‌زادگان مصری به نام خنوم‌هتپ دوم (Khnumhotep II) یافت شده است.

عبری‌ها در نوشتن کتاب مقدس ارمیای نبی، از یک شیوه رمزنگاری به نام Atbash استفاده می‌کردند، بدین‌سان که نام بسیاری از مکان‌ها و افراد در کتاب مقدس عبری‌ها عمداً با رمز Atbash به صورت مخفی و مبهم نوشته شده است. این رمز بسیار شبیه به رمز جانشینی است، بدین نحو که در Atbash اولین حرف از الفبای عبری با آخرین حرف جدول الفبا جانشین می‌شد. به همین نحو دومین حرف با حرف ما قبل آخر و این

روال به همین ترتیب تکرار می شد تا متن رمز شده به دست آید.

در یکی از شهرهای یونان باستان به نام اسپارتا، پیام‌ها از طریق نوشته شدن روی یک نوار کاغذی و پیچیدن آن دور یک استوانه‌ی با قطر مشخص رمزگذاری می‌شدند. نوار کاغذی تا زمانی که توسط گیرنده آن، روی یک استوانه با همان قطر قرار نمی‌گرفت، به صورت ناخوانا باقی می‌ماند. به این نوع از رمزنگاری اصطلاحاً آرشیلوس گفته می‌شد. جالب است بدانید که تا حدود پانصد سال راز این روش مخفی ماند تا عاقبت در ۱۲۰ قبل از میلاد راز این روش نگارش بر ملا شد.

در حوالی ۱۰۰ سال پیش از میلاد مسیح، ژولیس سزار (Julius Caesar)، در مکاتبات خود در هنگام جنگ از یک شیوه نوینی از رمزنگاری استفاده می‌کرد که در آن جای حروف الفبا تغییر پیدا می‌کرد. روش او در عین سادگی اما کارا و مفید بود، و عملاً اولین الگوی رمزنگاری ثبت شده در تاریخ به شمار می‌آید. در این الگو هر حرف با حرفی به فاصله  $n$  از خودش جانشین می‌شد. الگوی رمزنگاری ژولیوس سزار برای دورانی که از هر قوم و قبیله به ندرت کسانی با سواد بودند، به قدر کافی امنیت داشت ولی امروز بیشتر به یک شوخی شبیه است.

- [1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications, CRC Press, 1996.
- [2] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell system technical journal*, vol.28, no.4, pp.656–715, 1949.
- [3] M. Guizani, H. H. Chen, and C. Wang. *The Future of Wireless Networks: Architectures, Protocols, and Services*. Wireless Networks and Mobile Communications, Taylor & Francis, 2015.
- [4] A. Mason, S. C. Mukhopadhyay, and K. P. Jayasundera. *Sensing Technology: Current Status and Future Trends III*. Smart Sensors, Measurement and Instrumentation, Springer International Publishing, 2014.
- [5] S. Valenti, D. Rossi, A. Dainotti, A. Pescapè, A. Finamore, and M. Mellia, “Reviewing Traffic

- Classification,” in *Data Traffic Monitoring and Analysis SE - 6* (E. Biersack, C. Callegari, and M. Matijasevic, eds. ), vol.7754 of *Lecture Notes in Computer Science*, pp.123–147, Springer Berlin Heidelberg, 2013.
- [6] T. AbuHmed, A. Mohaisen, and D. Nyang, “A Survey on Deep Packet Inspection for Intrusion Detection Systems,” *Magazine of Korea Telecommunication Society*, vol.24, no.11, pp.25–36, 2008.
- [7] J. Muehlstein, Y. Zion, M. Bahumi, I. Kirshenboim, R. Dubin, A. Dvir, and O. Pele, “Analyzing {HTTPS} Encrypted Traffic to Identify User Operating System, Browser and Application,” *CoRR*, vol.abs/1603.0, 2016.
- [8] M. Crotti, M. Dusi, F. Gringoli, and L. Salgarelli, “Traffic classification through simple statistical fingerprinting,” *Computer Communication Review*, vol.37, pp.5–16, jan 2007.
- [9] M. Conti, J. Willemsen, and B. Crispo, “Providing source location privacy in wireless sensor networks: A survey,” *IEEE Communications Surveys and Tutorials*, vol.15, pp.1238–1280, jan 2013.
- [10] C. Ozturk, Y. Zhang, and W. Trappe, “Source-location privacy in energy-constrained sensor network routing,” in *Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and*

*Sensor Networks, SASN'04, SASN '04*, (New York, New York, USA), pp.88–93, ACM Press, 2004.

- [11] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, “A comprehensive survey of wireless body area networks,” *Journal of medical systems*, vol.36, no.3, pp.1065–1094, 2012.
- [12] M. B. Salem, S. Hershkop, and S. J. Stolfo, “A Survey of Insider Attack Detection Research,” in *Advances in Information Security*, vol.39, pp.69–70, Springer, 2008.

## A

AES ..... Advanced Encryption Standard

## D

DES ..... Data Encryption Standard



# واژه‌نامه انگلیسی به فارسی

## C

رمزنگاری ..... Cryptography

## S

امنیت ..... Security

# واژه‌نامه فارسی به انگلیسی

۱

امنیت ..... Security

د

رمزنگاری ..... Cryptography