به نام خداوند بخشنده مهربان

مبانی امنیت شبکه

Fundamentals of Network Security



یاشار ابری

دانشکده مهندسی، دانشگاه تهران

Yasharabri.ut.ac.ir@gmail.com

yasharabri@ut.ac.ir

۴

مبانی نظریه اعداد و آغاز استاندارد رمزنگاری پیشرفته (AES)

- سرفصل‌های این بخش:
  - یادآوری سریع نظریه اعداد و میدان‌های متناهی
  - چرا DES جایگزین شد و مسابقه NIST
  - ساختار کلی AES (Rijndael)

مبانی نظریه اعداد برای رمزنگاری

- **بخش‌پذیری و الگوریتم اقلیدس:** الگوریتم اقلیدس روشی کارآمد برای یافتن بزرگ‌ترین مقسوم‌علیه مشترک دو عدد است و پایه بسیاری از محاسبات کلید در RSA و AES است.
- **حساب پیمانه‌ای (Modular Arithmetic):** در این حساب، اعداد پس از رسیدن به یک مقدار مشخص (پیمانه) دوباره از صفر شمرده می‌شوند؛ همه عملیات رمزنگاری کلید عمومی بر پایه همین حساب انجام می‌شود.
- **گروه، حلقه و میدان:** این ساختارهای جبری، مجموعه‌ای از اعداد به‌همراه عملیات‌هایی مانند جمع و ضرب را با قوانین مشخص تعریف می‌کنند که پایه ریاضی رمزنگاری مدرن است.
- **میدان‌های متناهی GF(۲^n):** AES در سطح بایت با میدان متناهی GF(۲^۸) کار می‌کند که در آن هر بایت به‌عنوان یک چندجمله‌ای با ضرایب صفر و یک در نظر گرفته می‌شود؛ همین ساختار امکان طراحی جعبه جانشینی مقاوم AES را فراهم کرد.

حضرت رسول الله محمد مصطفی صلی الله علیه و آله و سلم:
همانا وصی من رازدار من بهترین بازماندگانم کسی که وعده‌ام را تحقق می‌بخشد و دِینم را ادا می‌کند علی بن ابیطالب است.
کنز العمال حدیث ۳۲۹۵۲

خاستگاه :AES چگونه جایگزین DES شد

- **نیاز به جایگزین:** پس از شکسته‌شدن عملی DES در ۱۹۹۸ و کندی/محدودیت‌های Triple DES، NIST در سال ۱۹۹۷ فراخوانی عمومی برای ارائه استاندارد رمزنگاری بعدی منتشر کرد.
- **فرایند رقابتی و شفاف:** برخلاف DES، این بار پانزده الگوریتم از سراسر دنیا رقابت کردند و کل فرآیند ارزیابی و تحلیل رمز به‌صورت عمومی و باز انجام شد تا اعتماد جامعه رمزنگاری جلب شود.
- **انتخاب نهایی: Rijndael:** در سال ۲۰۰۱، الگوریتم Rijndael که توسط دو رمزنگار بلژیکی به‌نام‌های وینسنت رایمن و یوان دیمن طراحی شده بود، به دلیل ترکیب امنیت بالا، سرعت و سادگی پیاده‌سازی به‌عنوان AES انتخاب شد.

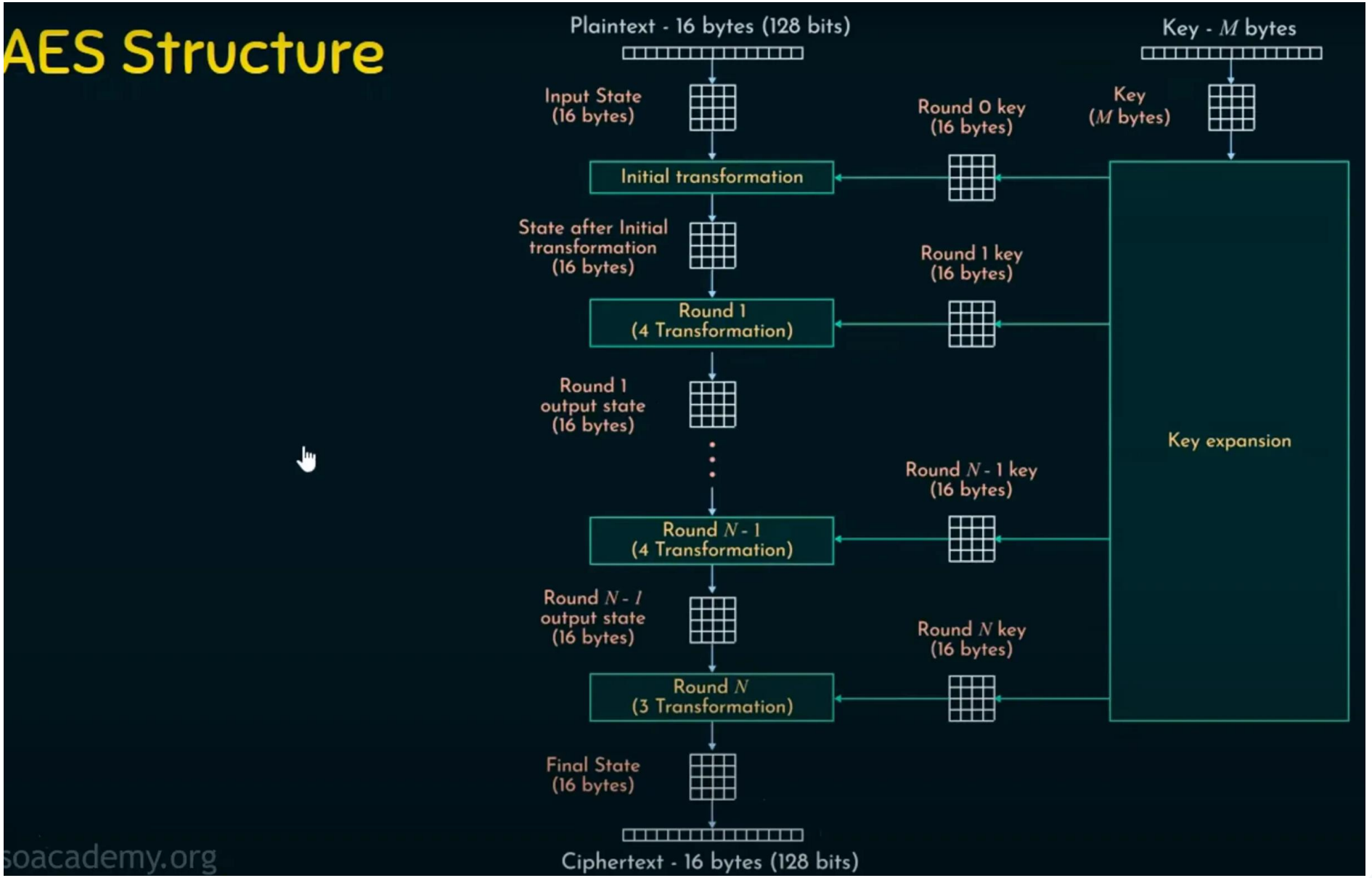
حضرت رسول الله محمد مصطفی صلی الله علیه و آله و سلم:
ای علی خداوند دوست داشتن مستمندان را به تو بخشیده است، از این رو آنان به پیشوای تو خرسندند و تو به داشتن پیروانی چون ایشان خرسندی.
ت دمشق جلد ۴۲ صفحه ۲۸۱

ساختار کلی AES

- **نوع ساختار:** برخلاف DES که شبکه فایستل بود، AES از یک شبکه جانشینی-جایگشتی (Substitution-Permutation Network) استفاده می‌کند که در آن کل بلوک در هر **دور**، هم **جانشین** و هم **جابه‌جا** می‌شود.
- **اندازه بلوک و کلید:** بلوک ورودی همیشه ۱۲۸ بیت است، اما طول کلید می‌تواند ۱۲۸، ۱۹۲ یا ۲۵۶ بیت باشد؛ طول کلید بزرگ‌تر به معنای تعداد دور بیشتر (به‌ترتیب ۱۰، ۱۲ یا ۱۴ دور) است.
- **ماتریس حالت (State):** داده ورودی به‌صورت یک ماتریس ۴ در ۴ از بایت‌ها نمایش داده می‌شود و تمام تبدیل‌های هر دور روی همین ماتریس اعمال می‌شوند.

حضرت امیرالمومنین امام علی بن ابیطالب صلوات الله علیه و آله:
بدان که مردم به چیزی مهم‌تر از تقوا سفارش نشده‌اند، چرا که این توصیه ما خاندان است.
وسائل جلد ۱۲ صفحه ۱۵۵

نمودار ماتریس بایتی AES و تبدیل اصلی هر دور



حضرت امام جعفر بن محمد صادق علیه السلام:

ارباب گونه به عیوب دیگران ننگرید، بلکه چون بنده‌ای متواضع عیب‌های خود را جستجو کنید.

تحف العقول صفحه ۲۹۵

رمزگذاری AES: ۱. تبدیل متن به ماتریس ۴×۴

- متن «HELLO AES WORLD!» به ۱۶ بایت تبدیل می‌شود و بایت‌ها طبق قرارداد AES، به ترتیب ستونی در ماتریس قرار می‌گیرند.

ماتریس متن اولیه

48	4F	53	52
45	20	20	4C
4C	41	57	44
4C	45	4F	21

- در این مرحله هنوز رمزگذاری انجام نشده است؛ فقط داده برای پردازش آماده می‌شود.

حضرت امام علی بن موسی الرضا علیه السلام: هر کس نتواند به زیارت من بیاید، برادرم در ری یا **خواهرم را در قم** زیارت کند. ثواب زیارت مرا می‌یابد.

زبده التصانیف جلد ۶ صفحه ۱۵۹

رمزگذاری AES: ۲. ترکیب با کلید اصلی

- هر بایت از ماتریس متن با بایت متناظر کلید اصلی، با عمل XORترکیب می‌شود. این مرحله آغاز رمزگذاری واقعی است.



- XORدو بیت را با هم مقایسه می‌کند: اگر متفاوت باشند خروجی ۱ و اگر یکسان باشند خروجی ۰ است.

حضرت امام علی بن موسی الرضا علیه السلام: سزاوار است که مرد در هزینه‌ها و خرجی به خانواده خود توسعه و گشایش دهد، تا آرزوی مرگش را نداشته باشند.
من لایحضر جلد ۲۳ صفحه ۶۸

رمزگذاری AES: ۳. تکرار دورهای اصلی ۱ تا ۹

- در هر یک از ۹ دور، چهار عملیات پشت سر هم انجام می‌شود: جایگزینی بایت‌ها (SubBytes)، چرخش سطرها (ShiftRows)، ترکیب ستون‌ها (MixColumns) و ترکیب با کلید همان دور (AddRoundKey). این دورها در اینجا یکجا خلاصه شده‌اند.

قبل از عملیات

0D	1F	12	19
1D	6C	65	09
0D	04	04	1D
01	65	6F	00

بعد از عملیات

F3	13	9C	86
46	E3	49	40
31	B2	5E	2F
02	7B	3B	58

- برای کوتاه ماندن آموزش، جزئیات هر دور جداگانه نمایش داده نمی‌شود. ماتریس سمت راست، حالت واقعی پس از پایان دور ۹ است؛ در اجرای واقعی، کلیدهای دور K۱ تا K۹ به‌ترتیب استفاده می‌شوند.

حضرت امام موسی بن جعفر کاظم علیه السلام: امانت داری و راستی، روزی آور است و خیانت و دروغ فقر و نفاق می‌آورد. تحف العقول صفحه ۴۰۳

رمزگذاری AES: ۴. دور نهایی (دور ۱۰)

- در دور آخر، ابتدا بایت‌ها جایگزین و سطرها چرخانده می‌شوند؛ سپس حالت با کلید دور ۱۰ ترکیب می‌شود. برخلاف دورهای ۱ تا ۹، در دور آخر MixColumns انجام نمی‌شود.



- سه عملیات این دور در یک گام نمایش داده شده‌اند تا تعداد مراحل کم بماند.

حضرت امام علی بن موسی الرضا علیه السلام: کسی که از انسان‌های نیکوکار تشکر و قدردانی نکند از خداوند سبحان هم قدردانی نکرده است.

بحار جلد ۷۱ صفحه ۴۴

رمزگذاری AES: ۵. متن رمزشده

- خروجی نهایی، ۱۶ بایت رمزشده است. بدون کلید صحیح، از روی این خروجی نباید بتوان متن اصلی را به‌سادگی تشخیص داد.

ماتریس متن رمزشده

3C	44	8C	B9
8B	75	AE	94
D5	80	15	2A
7C	25	CF	7D

متن رمزشده به شکل هگزادسیمال: C۸BD۵۷C۴۴۷۵۸۰۲۵۸CAE۱۵CFB۹۹۴۲A۷D۳

حضرت امام محمد بن علی جوادالائمه علیه السلام:
هرکس بدون آگاهی کاری انجام دهد، بیشتر از آنکه درست کند خراب می‌کند.
بحارالانوار جلد ۷۸ صفحه ۳۴۶

رمزگشایی AES: ۱. دریافت متن رمزشده

- ۱۶ بایت متن رمزشده دریافت و با همان قرارداد ستونی AESدر ماتریس ۴×۴ قرار داده می‌شود.

ماتریس متن رمزشده

3C	44	8C	B9
8B	75	AE	94
D5	80	15	2A
7C	25	CF	7D

- رمزگشایی از ماتریس رمزشده آغاز می‌شود و عملیات معکوس را اجرا می‌کند.

حضرت امام محمد بن علی باقر علیه السلام: افزایش نعمت از طرف خداوند قطع نمی‌شود، مگر به خاطر ناسپاسی بندگان.

بحارالانوار جلد ۷۱ صفحه ۵۵

رمزگشایی AES: ۲. ترکیب با کلید دور ۱۰

- ابتدا ماتریس رمزشده با کلید دور ۱۰ توسط XOR ترکیب می‌شود. این کار نخستین گام معکوس در AES است.

قبل از عملیات

3C	44	8C	B9
8B	75	AE	94
D5	80	15	2A
7C	25	CF	7D

کلید دور ۱۰ (K۱۰)

31	39	52	FD
9A	4E	A7	CE
8D	95	D2	1D
16	52	EE	9F

برای مرحلهٔ AddRoundKey

بعد از عملیات

0D	7D	DE	44
11	3B	09	5A
58	15	C7	37
6A	77	21	E2

- در رمزگشایی، کلیدهای دور از آخر به اول استفاده می‌شوند.

حضرت امام جعفر بن محمد صادق علیه السلام: عید غدیر روز عید، خوشی، شادی است و روز روزه‌داری به عنوان سپاس نعمت الهی است. وسائل الشیعه جلد ۷ صفحه ۳۲۶

رمزگشایی AES: ۳. دورهای معکوس ۹ تا ۱

- در هر دور معکوس، عملیات وارون اجرا می‌شوند: چرخش معکوس سطرها، جایگزینی معکوس بایت‌ها، ترکیب با کلید همان دور و ترکیب معکوس ستون‌ها. این دورها از ۹ به ۱ طی می‌شوند و در اینجا یکجا خلاصه شده‌اند.

قبل از عملیات

0D	7D	DE	44
11	3B	09	5A
58	15	C7	37
6A	77	21	E2

بعد از عملیات

D7	C0	C9	D4
50	4D	01	A4
F2	A4	D7	F2
63	7C	4D	A8

- ماتریس سمت راست، حالت واقعی پس از پایان دور معکوس ۱ است. در نمایش فشرده، جزئیات هر دور جداگانه باز نشده‌اند.

حضرت امام جعفر بن محمد صادق علیه السلام: روز غدیر خم در میان روزهای عید فطر، قربان و جمعه همانند ماه در میان ستارگان است.
اقبال سید صفحه ۴۶۶

رمزگشایی AES: ۴. پایان رمزگشایی با کلید اصلی

- در گام پایانی، چرخش معکوس سطرها و جایگزینی معکوس بایت‌ها انجام می‌شود و در پایان، XORبا کلید اصلی K_0متن را به حالت اولیه بازمی‌گرداند.

قبل از عملیات

D7	C0	C9	D4
50	4D	01	A4
F2	A4	D7	F2
63	7C	4D	A8

کلید اصلی (K_0)

45	50	41	4B
58	4C	45	45
41	45	53	59
4D	20	20	21

برای مرحلهٔ AddRoundKey

بعد از عملیات

48	4F	53	52
45	20	20	4C
4C	41	57	44
4C	45	4F	21

- عملیات معکوس در جهت مخالف رمزگذاری انجام می‌شوند؛ به همین دلیل متن اصلی بازیابی می‌شود.

حضرت امام علی بن محمد هادی علیه السلام: خود بزرگ بینی انسان را از دانش آموختن باز می‌دارد و او را به نادانی و پستی می‌کشاند.

اعیان الشیعه جلد ۲ صفحه ۳۹

رمزگشایی AES: ۵. متن سادهٔ بازیابی‌شده

- با خواندن بایت‌های ماتریس نهایی، متن سادهٔ اولیه دوباره به دست می‌آید.

ماتریس متن بازیابی‌شده

48	4F	53	52
45	20	20	4C
4C	41	57	44
4C	45	4F	21

- متن بازیابی‌شده: HELLO AES WORLD! – با ورودی اولیه یکسان است.

حضرت صاحب الامر امام عصر عجل الله تعالی فرجه الشریف:
هر صبح و شام بر تو گریه و شیون می‌کنم و در مصیبت تو به جای اشک خون می‌گریم.
بحارالانوار جلد ۱۰۱ صفحه ۲۳۸