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

۹

توابع درهم‌ساز رمزنگاری

- سرفصل‌های این بخش:
  - کاربردها و الزامات امنیتی توابع Hash
  - خانواده SHAو فروپاشی SHA-۱
  - چرا SHA-۳با ساختار متفاوت طراحی شد

کاربردها و الزامات توابع درهم‌ساز

- **تعریف:** تابع درهم‌ساز، ورودی با طول دلخواه را به یک خروجی با طول ثابت (چکیده یا Hash) تبدیل می‌کند و این فرایند یک‌طرفه است، یعنی از روی خروجی نمی‌توان ورودی را بازسازی کرد.
- **مقاومت در برابر برخورد:** یک تابع Hash خوب باید طوری طراحی شود که یافتن دو ورودی متفاوت با یک خروجی یکسان (برخورد) از نظر محاسباتی تقریباً غیرممکن باشد.
- **کاربردهای کلیدی:** تأیید یکپارچگی فایل دانلودشده، تولید امضای دیجیتال (چون امضا کردن چکیده کوچک به‌جای کل پیام بسیار سریع‌تر است)، تولید MAC و ذخیره امن رمز عبور به‌جای متن ساده آن.

امیرالمومنین علی علیه السلام:
دلت را با اندرز زنده بدار.
نهج البلاغه، نامه ۳۱

MAC آدرس چیست

- MAC آدرس، آدرس فیزیکی یک دستگاه است که به طور منحصر به فرد آن را در یک شبکه خاص شناسایی می‌کند. MAC مخفف Media Access Control است و به آن آدرس سخت افزاری، آدرس فیزیکی نیز گفته می‌شود.
- مک آدرس یک عدد هگزادسیمال ۱۲ رقمی است که به هر دستگاه متصل به شبکه اختصاص داده می‌شود.
- آدرس MAC که عمدتاً به عنوان یک شناسه در طول ساخت دستگاه مشخص می‌شود، اغلب در کارت رابط شبکه (NIC) دستگاه یافت می‌شود.
- هنگام تلاش برای مسیریابی دستگاه و یا هنگام عیب‌یابی در دستگاه شبکه، آدرس MAC مورد نیاز است.
- ممکن است یک دستگاه بیش از یک آدرس MAC داشته باشد. به عنوان مثال، اگر لپ‌تاپ دارای پورت کابل Ethernet و WiFi داخلی باشد، دو آدرس مک در پیکربندی سیستم نشان داده می‌شود.

امام صادق علیه السلام: معاشرت و رفت و آمد با خویشاوندان، حساب روز قیامت را بر انسان آسان می‌کند.

بحارالانوار: ج۷۴، ص۱۰۲

دسیمال (مبنای ۱۰ یا ده‌دهی) و هگزادسیمال (مبنای ۱۶)

Decimal	Hexadecimal
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

امام علی علیه السلام:

مرد به کردارش آزموده می شود، نه به گفتارش.

غرر الحکم، ح۱۱۰۲۶

هگزادسیمال (مبنای ۱۶)



تمامی کاراکترهایی که در تصویر مشاهده می‌کنید بیانگر عدد هستند!

امام هشتم(ع) به نقل از پدران بزرگوارش فرمود: رسول خدا صلی الله علیه و آله فرمود: برترین اعمال امّت من انتظار فرج از خدای عزوجل می باشد. بحارالأنوار، ج ۵۲، ص ۱۲۲.

خانواده SHA و ساختار Merkle-Damgård

- **ساختار زنجیره‌ای:** الگوریتم‌های SHA-۱ و SHA-۲ پیام را به بلوک‌های ثابت تقسیم کرده و هر بلوک را به‌همراه خروجی بلوک قبلی پردازش می‌کنند تا در پایان یک چکیده نهایی تولید شود.
- **عمر SHA-۱:** NIST این الگوریتم را در سال ۱۹۹۵ استاندارد کرد، اما پژوهشگران به‌تدریج ضعف‌های نظری آن را نشان دادند تا این‌که در سال ۲۰۱۷ تیمی از گوگل و CWI هلند نخستین برخورد عملی واقعی را با نام «SHAttered» ساختند و عملاً استفاده از SHA-۱ را برای کاربردهای امنیتی پایان دادند.
- **جایگزین: SHA-۲ :** خانواده SHA-۲ (شامل SHA-۲۵۶ و SHA-۵۱۲) با اندازه چکیده بزرگ‌تر و تغییرات ساختاری، همچنان امن است و امروزه پرکاربردترین تابع Hash در پروتکل‌های اینترنتی است.

امیرالمومنین علی علیه السلام : نماز، دژ محکم خداوند مهربان و وسیله راندن شیطان است.
غررالحکم، ح ۲۲۱۳

چرا SHA-۳ ساخته شد؟

- **نگرانی NIST**: با وجود امن‌بودن SHA-۲، نگرانی این بود که چون SHA-۲ از همان خانواده ساختاری SHA-۱ است، اگر روزی یک حمله ساختاری کشف شود، هر دو خانواده هم‌زمان آسیب‌پذیر می‌شوند.
- **مسابقه عمومی:** NIST طی سال‌های ۲۰۰۷ تا ۲۰۱۲ مسابقه‌ای مشابه AES برگزار کرد و در پایان الگوریتم Keccak، طراحی‌شده توسط تیمی از رمزنگاران بلژیکی و ایتالیایی، برنده شد.
- **ساختار اسفنجی (Sponge):** برخلاف ساختار زنجیره‌ای SHA-۲، Keccak داده را در یک حالت داخلی بزرگ 'جذب' کرده و سپس خروجی را از همان حالت 'می‌فشارد'؛ این تفاوت بنیادی ساختاری باعث می‌شود ضعف احتمالی SHA-۲ روی SHA-۳ اثر نگذارد.

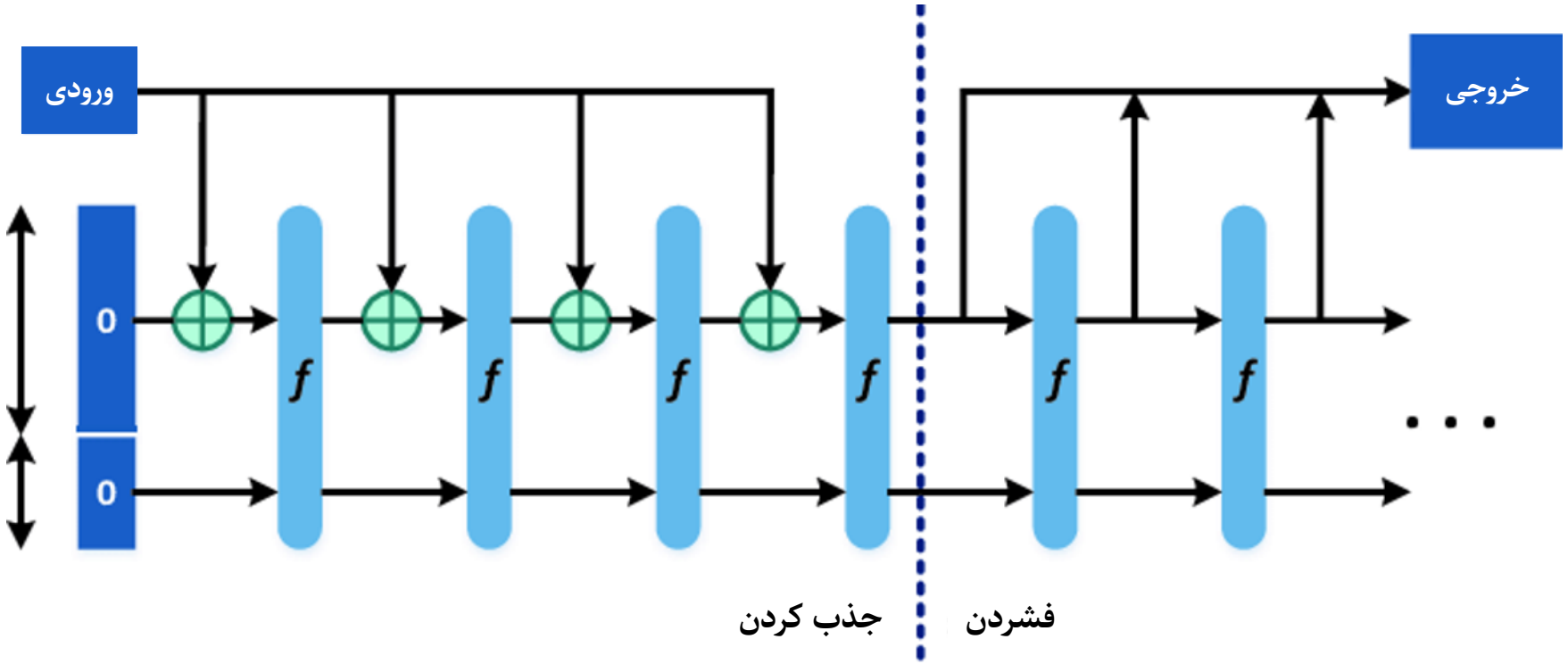
امیرالمومنین علی علیه السلام:
خدا را، خدا را درباره نماز، که بهترین کردار و ستون دین شماست!
گزیده تحف العقول، ح۶۵

ساختار اسفنجی (Sponge) در الگوریتم Keccak

- برای درک ساختار اسفنجی، تصور کنید یک اسفنج داریم که ابتدا آب را به خود جذب می‌کند و سپس با فشردن آن، آب را خارج می‌کند.
- الگوریتم Keccak نیز تقریباً با همین ایده کار می‌کند؛ با این تفاوت که به‌جای آب، داده‌های ورودی را دریافت می‌کند و به‌جای آب خارج‌شده، خروجی هش را تولید می‌کند.
- این ساختار دو مرحله اصلی دارد:
  - ۱. مرحله جذب (Absorbing)
  - ۲. مرحله فشردن (Squeezing)

امام صادق علیه السلام:
خوش‌خویی گناه را ذوب می‌کند، همچنان که آفتاب یخ را.
الکافي: ج۲، ص۱۰۰، ح۷

ساختار اسفنجی Keccak با فازهای جذب (Absorbing) و فشردن (Squeezing)



پیامبر خدا صلی الله علیه و آله :

اگر می توانید هر روز را نوروز کنید؛ یعنی در راه خدا به یکدیگر هدیه بدهید و با یکدیگر پیوند داشته باشید.

دعائم الإسلام: ج۲، ص۳۲۶

ساختار اسفنجی Keccak : فاز جذب (Absorbing)

- **۱. مرحله جذب (Absorbing)**
  - در این مرحله، پیام ورودی به الگوریتم داده می‌شود.
  - **۱. تقسیم پیام:** پیام ورودی به چند بلوک کوچک‌تر تقسیم می‌شود.
  - **۲. ورود بلوک اول:** اولین بلوک پیام وارد حالت داخلی (State) الگوریتم می‌شود.
  - **۳. ترکیب و پردازش:** داده ورودی با بخشی از حالت داخلی ترکیب می‌شود و سپس تابع تبدیل f روی کل حالت داخلی اجرا می‌شود.
  - **۴. تکرار:** بلوک بعدی وارد می‌شود و دوباره تابع f اجرا می‌شود. این کار تا زمانی ادامه پیدا می‌کند که تمام بلوک‌های پیام جذب شوند.
  - در واقع، هر بلوک ورودی روی وضعیت داخلی الگوریتم تأثیر می‌گذارد و آن را تغییر می‌دهد.

حضرت محمد صلی الله علیه و آله:
داناترین مردم کسی است که دانش مردم را با دانش خود جمع کند.
أمالي، صدوق: ۷۳/۴۱

ساختار اسفنجی Keccak: فاز فشردن (Squeezing)

- **۲. مرحله فشردن (Squeezing)**
  - پس از جذب تمام پیام، الگوریتم وارد مرحله تولید خروجی می‌شود.
  - **۱. شروع تولید خروجی:** بخشی از حالت داخلی فعلی به‌عنوان خروجی هش استخراج می‌شود.
  - **۲. تولید خروجی بیشتر:** اگر طول خروجی موردنیاز هنوز تأمین نشده باشد، تابع تبدیل f دوباره روی حالت داخلی اجرا می‌شود.
  - **۳. استخراج مجدد:** پس از پردازش، بخش دیگری از حالت داخلی استخراج می‌شود.
  - **۴. تکرار:** این کار تا رسیدن به طول خروجی موردنظر ادامه پیدا می‌کند.

پیامبر خدا صلی الله علیه و آله:
استوارترین شما بر صراط، کسی است که علاقه‌اش نسبت به من و اهل بیتم بیشتر باشد.
جامع الأحادیث قمّي، ص۲۳۱

تفاوت دو مرحله در یک نگاه

مرحله	عملکرد
جذب (Absorbing)	دریافت بلوک‌های پیام و ترکیب آن‌ها با حالت داخلی
فشردن (Squeezing)	استخراج بخش‌هایی از حالت داخلی برای تولید خروجی هش

امیرالمومنین علی علیه السلام:
در تصمیمی که با دور اندیشی همراه نباشد خیری نیست.
غرر الحکم، ح ۱۰۶۸۲