### ****قدرت پردازشی CPU و GPU در حملات Brute-Force****

حمله **Brute-Force** وابسته به تعداد محاسباتی است که سخت‌افزار می‌تواند در هر ثانیه انجام دهد. دو عامل اصلی در این زمینه عبارتند از:

**سرعت پردازش (FLOPS)**: تعداد عملیات محاسباتی ممیز شناور در ثانیه.

**سرعت و معماری موازی‌سازی**: مخصوصاً در GPU که عملیات موازی در مقیاس وسیع انجام می‌شود.

#### **نمونه‌ای از CPU مدرن:**

* **AMD Ryzen 9 7950X**
  + **هسته‌ها/رشته‌ها**: 16 هسته / 32 رشته
  + **فرکانس پایه/توربو**: 4.5 گیگاهرتز / 5.7 گیگاهرتز
  + **قدرت پردازشی**: حدود 59 ترافلاپس (TFLOPS) برای محاسبات ممیز شناور 32 بیتی.
  + **کاربرد در Brute-Force**: این CPU می‌تواند در حدود **10-15 میلیارد هش در ثانیه** برای الگوریتم‌های مانند MD5 تولید کند.

#### **نمونه‌ای از GPU مدرن:**

* **NVIDIA GeForce RTX 4090**
  + **هسته‌های CUDA**: 16,384
  + **فرکانس بوست**: تا 2.52 گیگاهرتز
  + **قدرت پردازشی**: حدود 82.6 ترافلاپس برای محاسبات FP32.
  + **کاربرد در Brute-Force**: با استفاده از نرم‌افزارهایی مانند Hashcat می‌تواند حدود **300-400 میلیارد هش در ثانیه** برای الگوریتم MD5 یا حدود **70-100 میلیارد هش در ثانیه** برای SHA-256 انجام دهد.

### ****2. مقایسه با ابرکامپیوترهای پیشرفته:****

ابرکامپیوترهایی مانند **Frontier** از معماری‌های متفاوت برای انجام محاسبات در مقیاس بزرگ استفاده می‌کنند:

* **Frontier ساخت( AMD و HPE** ):
  + قدرت پردازشی: **1.1 اگزافلاپس** (10^18 عملیات در ثانیه)
  + کاربرد: انجام میلیون‌ها محاسبه موازی برای پروژه‌های علمی و شبیه‌سازی.
  + **در حملات Brute-Force**: اگر بهینه‌سازی شود، Frontier می‌تواند **میلیاردها میلیارد هش در ثانیه** انجام دهد، اما این نوع استفاده معمولاً برای چنین سیستم‌هایی کاربرد ندارد.

### ****3. معیارهای عملکردی (Benchmark):****

معیارهایی که برای اندازه‌گیری عملکرد CPU و GPU در حملات Brute-Force استفاده می‌شود، معمولاً بر اساس الگوریتم‌های رمزنگاری و نرم‌افزارهای خاص تعیین می‌گردد:

* **MD5 یا SHA-1**: برای هش‌های ساده.
* **SHA-256 یا bcrypt**: برای الگوریتم‌های مقاوم‌تر.

#### **مثال نرم‌افزار: Hashcat**

* **AMD Ryzen 9 7950X**: حدود 12 میلیارد هش در ثانیه برای MD5.
* **NVIDIA RTX 4090**: حدود 300 میلیارد هش در ثانیه برای MD5.

### ****جمع‌بندی:****

1. پردازنده‌های CPU و GPU مدرن می‌توانند میلیاردها هش در ثانیه تولید کنند. به عنوان مثال، RTX 4090 حدود 300 میلیارد هش در ثانیه برای MD5 انجام می‌دهد.
2. قدرت ابرکامپیوترها مانند Frontier با 1.1 اگزافلاپس بسیار بیشتر است، اما معمولاً برای کاربردهای دیگر طراحی شده‌اند.
3. حملات Brute-Force به قدرت سخت‌افزار، الگوریتم هدف، و روش بهینه‌سازی بسیار وابسته است. برای الگوریتم‌های مقاوم‌تر، زمان حمله به‌شدت افزایش می‌یابد.