تولد باقر

صابر و جابر و باقر ۳ دوست قدیمی هستند. تولد باقر نزدیک است و صابر و جابر می‌خواهند که برای تولد باقر، او را غافلگیر کنند. اما به علت کرونا، تا خود روز تولد نمی‌خواهند بیرون از خانه بروند و یکدیگر را ببینند. پس مجبورند به صورت غیرحضوری هماهنگی‌های لازم را انجام دهند. باقر رئیس شرکت باتل (bottle، مخفف باقر تل) است که اپراتورهای تلفن همراه صابر و جابر می‌باشد. باقر دوست دارد قبل از تولدش بداند که صابر و جابر برای او چه کادویی می‌خرند، برای همین پیامک‌های آن‌ها را شنود می‌کند. به همین علت صابر و جابر مجبورند از یک پروتکل برای رمزنگاری پیام‌های خود استفاده کنند. آن‌ها پروتکل AES را برای رمزنگاری پیام‌های خود انتخاب می‌کنند. در پیاده‌سازی الگوریتم رمزنگاری AES128، به آن‌ها کمک کنید.

نکات پیاده‌سازی

دقت کنید که برای پیاده‌سازی نمی‌توانید از کتابخانه‌هایی که به صورت آماده این پروتکل را پیاده‌سازی کرده‌اند استفاده کنید.

برای پیاده‌سازی بخش SBox از Lookup Table استفاده کنید.

ورودی

در ورودی ابتدا کلید و سپس متنی که باید رمز شود در دو خط جداگانه و به صورت عدد هگزادسیمال وارد می‌شود. تضمین می‌شود که کلید و متن ۱۲۸ بیتی هستند.

خروجی

در خروجی باید متن رمز شده به صورت هگزادسیمال چاپ شود.

ورودی نمونه

```
c0000000000000000000000000000000
00000000000000000000000000000000
```

خروجی نمونه

```
4bc3f883450c113c64ca42e1112a9e87
```

حالا خودمون چکار کنیم؟

پس از اینکه صابر و جابر موفق شدند پیام‌های خود را با الگوریتم AES رمز کنند، حالا باید بتوانند پیام‌های یکدیگر را رمزگشایی کنند تا قابل خواندن باشد. در پیاده‌سازی الگوریتم رمزگشایی AES128، به آن‌ها کمک کنید.

ورودی

در ورودی ابتدا کلید و سپس متن رمز شده در دو خط جداگانه و به صورت هگزادسیمال وارد می‌شود. تضمین می‌شود که کلید و متن رمز شده ۱۲۸ بیتی هستند.

خروجی

در خروجی باید متن رمزگشایی شده به صورت هگزادسیمال چاپ شود.

ورودی نمونه

```
80000000000000000000000000000000
0edd33d3c621e546455bd8ba1418bec8
```

خروجی نمونه

```
00000000000000000000000000000000
```

کلیدساز

متاسفانه باقر متوجه شده که صابر و جابر می‌خواهند از پروتکل AES برای رمزنگاری استفاده کنند و می‌خواهد هنگام تبادل کلید، کلید آن‌ها را شنود کرده و پیام‌های آن‌ها را رمزگشایی کند، برای همین صابر و جابر باید به نحوی کلید را منتقل کنند که باقر نتواند پیام‌های آن‌ها را رمزگشایی کند. آن‌ها می‌خواهند برای اینکار از پروتکل دفی – هلمن استفاده کنند. در پیاده‌سازی الگوریتم دفی – هلمن، به آن‌ها کمک کنید.

دقت کنید که اعداد شما ممکن است در متغیرهای عادی ذخیره نشوند (مقدار آن‌ها بزرگ باشد).

ورودی

در ورودی به ترتیب p (مقدار پیمانه یا مشخصه میدان)، g (مولد گروه)، a (متغیر تصادفی برای صابر) و b (متغیر تصادفی برای جابر) از ورودی گرفته می‌شوند.

خروجی

در خروجی باید به ترتیب کلید صابر، کلید جابر و عددی که باقر به عنوان کلید می‌بیند در یک خط چاپ شود.

ورودی نمونه

```
541 10 123 34
```

خروجی نمونه

```
384 398 93
```

برای گرفتن نمونه‌های بیشتر می‌توانید از وبسایت زیر استفاده کنید.

https://www.irongeek.com/diffie-hellman.php