No Leaks

זה מרגיש כמו צאלנג קצת מצחיק, אולי אני מבין לא נכון

אבל בכל בקשה אני פוסל 20 בתים מהciphertext של הדגל

בפרט, לכל בית בפאלג יש 255 אופציות, בכל פעם שחוזר לי ct תקין אני מוריד אופציה נוספת.

למה לא פשוט לנסות עד שהאופציות נגמרות?

הלכתי על 1000 בקשות וזה מה שנשאר עבור כל תו

```
{99, 80, 178, 26, 251, 158}
{36, 228, 167, 233, 74, 202, 114, 148, 53, 118, 217, 95}
{224, 8, 41, 200, 139, 17, 146, 245, 121, 30, 255}
{112, 170, 12}
{35, 73, 172, 51, 116, 148, 54, 24, 253, 61}
{1, 225, 200, 234, 111}
{131, 142, 239, 117, 123, 63}
{132, 73, 10, 170, 173, 209, 117, 53, 26}
{67, 140, 110, 144, 91, 126}
{102, 7, 75, 48, 82, 114}
{107, 205, 208, 114, 178, 52, 181, 119, 56, 185}
{7, 109, 110, 144, 85, 150, 27, 93}
{72, 134, 100, 102}
{131, 101, 203, 48, 112, 176, 22, 153, 61}
{65, 109, 233, 21}
{161, 228, 230, 111, 95, 223}
{121, 163, 218, 48, 117, 25, 186}
{225, 233, 13, 127, 47, 92, 112, 55, 60, 63}
{102, 103, 8, 137, 112, 125, 245, 254, 61, 222}
{34, 167, 39, 235, 205, 178, 125}
```

נדיר – את ה7 הראשונים אני כבר יודע (וגם את האחרון), זה משאיר 13 תווים עם בערך 7 אופציות לתו?

לא פיזבילי (אם אני לא טועה זה 13^7, זה 62 מיליון איטרציות, אפשרי אבל כואב, עוד 1000 בקשות ייקח משמעותית פחות זמן, במיוחד אם הייתי ממקבל)

ו... פוצח

```
100%
{99}
{114}
{121}
{112}
{116}
{111}
{122, 123, 191}
{208, 117}
{155, 110}
{114}
{52}
{110}
{100}
{48, 224, 151}
{109, 101}
{95}
{48}
{55}
{112}
{125}
```

עכשיו אריץ עם הדפסה נורמלית ו2048 איטרציות, בתקווה שהריצה תלך טובה כמו הקודמת (ואם לא אז פשוט אצליב)

```
crypto{{'u', '8'}{'\x95', 'n'}r4{'\x11', 'n'}d0m_07p}
```

crypto{unr4nd0m_07p}