13.18 Aufgabe: Cut-and-Paste Angriff auf ECB

Der Plaintext sei

```
Money_for_Alice_is_$1000
Money_for_Trudy_is_$2___
```

wobei _ das Leerzeichen ist.

Angenommen die Angreiferin Trudy weiß,

- dass der ECB Modus verwendet wird
- wie die generelle Struktur des Plaintexts aussieht
- dass Sie nur $2 erhalten wird
- dass in 64 Bit-Blöcken verschlüsselt wird
- dass ein Buchstabe in 8 Bit verschlüsselt wird

Beschreiben Sie, wie Trudy einen Cut-and-Paste Angriff durchführen würde, um den ihr zukommenden Geldbetrag zu erhöhen.

Sie könnte die letzten 3 Zeichen, also die letzten 24 bit von Alice kopieren und bei ihr austauschen. Also würde sie dann 2000 $ bekommen. Vorausgesetzt das Trudy irgendwie die Verschlüsselung abfangen und manipulieren kann, weil sie ins Tutorium von Prof Knorr gegangen ist.