Quiz 2.17

Q:1A

* Double DES → use 2 DES encrypts on each block
  → $C = E_{K_2}(E_{K_1}(P))$

$P \rightarrow [E_{K_1}] \rightarrow [E_{K_2}] \rightarrow C$

* Triple DES → use 2 keys with E-D-E sequence
  → $C = E_{K_1}(D_{K_2}(E_{K_1}(P)))$

$P \rightarrow [E_{K_1}] \rightarrow [D_{K_2}] \rightarrow [E_{K_1}] \rightarrow C$

* Triple DES is more secure, as double DES is vulnerable to the "meet-in-the-middle" attack, since $X = E_{K_1}(P) = D_{K_2}(C)$. ①

Moreover, it can be reduced to a single stage DES which is very vulnerable!

Q:1b 220 encry/sec, key size = 40 bits
↳ Assume same Rate for the decryption! → 19.008×10^6 decry/day

time Rel ⇒ $2^{40} / 19.008 \times 10^6 \approx 57'844.6$ days
$\approx$ **158.47** years

* Bruteforce attack would be practical if we have much faster CPU OR the key size is really small, unless that happens, the brute force attack is not practical at all!

* The attack will still be useless!

1-C 112-bit DES VS 56bit DES !

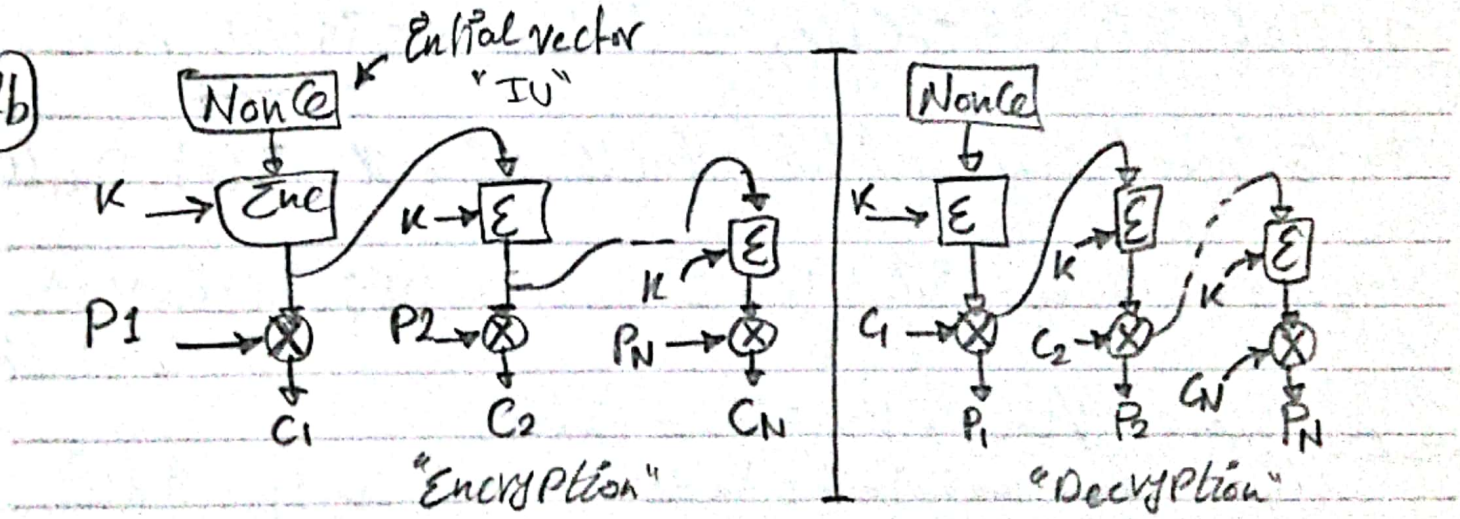
* The key-space sizes are 2^{112} VS. 2^{56}. Hence, the ratio of the time would be sth like: $2^{112}/2^{56} = 2^{56} \approx 7 * 10^{16}$

Q.2a

Stream ciphers → | Block ciphers →

1) output Feedback (OFB)
2) Cipher Feedback (CFB)
3) Counter (CTR)
4) Electronic Codebook (ECB)
5) cipher block chaining (CBC)

2b



2C Adv → Bit Errors don't Propagate

Disadv →
- Need an IV which is unique for each use
- Sender & receiver must remain in sync
- More vulnerable to message stream modification
- only used with "Full Block Feedback" ie CFB-64, CFB-128