Block Ciphers vs. Encryption

Last Time:  \( F \) is a block cipher \( \iff \)

\[
F(k, -) , \text{ for random } k
\]

"looks like" a randomly chosen permutation over \( \mathcal{S}_n \)

What is "encryption"?

secure communication
should hide information about plaintext

\( \downarrow ? \)

Definitely, shouldn't be able to determine plaintext from ciphertext (w/o exponential effort)

Is that all we need?  (No)

Q: Is a block cipher an encryption scheme?

i.e., \( F(k, m) = c \) is "encryption"?

Adobe Password Leak:

"encrypted" each password by sending it through block cipher

"ECB mode" = chop up data into chunks of the block-length (and pad the last block w/ 0's / null chars)
Leaks information:
when 2 blocks of input are identical, their ciphertext blocks are identical.

It seems like insignificant information leakage but it's very serious!

Design goal for encryption:
should not leak any partial information (so can be useful in any system)

Semantic security / Chosen Plaintext Attack (CPA) security
game between Adv & challenger

Challenger picks encryption key k
Adv can ask for any m, gets back Enc(k,m)

"Challenge step"

\[
\begin{cases}
\text{Adv chooses plaintexts } m_0, m_1, \\
\text{challenger flips coin} \\
\text{if heads, send back } Enc(k, m_0) \\
\text{if tails, send back } Enc(k, m_1)
\end{cases}
\]

Adv can ask for any m, gets back Enc(k,m)
Adv guesses coin

⇒ CPA security ⇐ guessing correctly w/ prob > \frac{1}{2}

is computationally hard problem.

Q: What happens if Adv asks same m to be encrypted twice in this game?

\[
\begin{cases}
\text{Ask for } m_0, m_1, \text{ in challenge phase} \\
\text{Ask for } m_0, m_1, \text{ again (separately) later or} \\
\text{if } Enc(k,m_0) \text{ always gives same result,} \\
\text{then Adv can guess correctly coin}
\end{cases}
\]

Implication: To be CPA-secure, calling Enc(k,m)
on same thing twice must give different results

⇒ Enc must be randomized (in addition to
random choice of k)

⇒ Dec must decrypt all possibilities correctly