PKI and Diffie-Hoffman Notes

These notes are about different notation that is used in notes and class and possibly in different quiz or exams.

In PKI, you have a **Public** key and a **Private** key. In the notes that is on Moodle and List machine **U** is used for Public and **R** is used for **Private**. Where as in class we used \( K^+ \) for public and \( K^- \) for private.

Thus,

\[
Y = E[PU_a, X] \quad == \quad Y = K^+_A(X) \quad \text{Encoding of message } X
\]

\( a \) and \( A \) both denotes the same person \( A \) or Alice

\[
X = D[PR_a, X] \quad == \quad X = K^-_A \quad \text{decoding of encrypted text } Y
\]

\[
Y = E[PR_b, X] \quad == \quad Y = K^-_B(X) \quad \text{Encryption of } X \text{ by Bob's private key}
\]

\[
X = D[PU_b, Y] \quad == \quad X = K^+_B(Y) \quad \text{Decryption of } Y \text{ by Bob's public key}
\]

Note that \( K^+ \) and \( K^- \) are inverses of each other:

\[
K^+_A(K^-_A(x)) = x \quad \forall x \text{ and } \forall A
\]

\[
K^-_A(K^+_A(x)) = x \quad \forall x \text{ and } \forall A
\]

Diffie-Hoffman

Let \( a \) be primitive root of unity. In notes \( \alpha \) is used for \( a \). Just notice that both are same in these formulas.