PKI and Diffie-Hoffman Notes

These notes is 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 Liste machine **U** is used for Public and **R** is used for P**R**ivate. Where as in class we used K^+ for public and K^- for private.

Thus,

$$Y = E[PU_a, X] \quad == \quad Y = K_A^+(X) \quad \text{Encoding of mesage X}$$

a and **A** both denotes the same person A or Alice

$$X = D[PR_a, X] \quad == \quad X = K_A^- \quad \text{decoding of encripted text Y}$$

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

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

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

$$K_A^+(K_A^-(x) = x \qquad \forall x \text{ and } \forall A$$

$$K_A^-(K_A^+(x) = x \qquad \forall x \text{ and } \forall A$$

Diffie-Hoffman

Let a be primitive root pf unity. In notes α is used for a. Just notice that both are same in these formulas.