S T Q Q S S D __/__/__

Trabalho Final - Criptografia

6) a) $\begin{cases} X \equiv a \pmod p \\ X \equiv b \pmod q \end{cases}$ $X \equiv (a \cdot q \cdot q') + (b \cdot p \cdot p') \pmod N$.

Sendo que $mdc(p, q) = 1$

Teorema: O sistema $\begin{cases} X \equiv a \pmod p \\ X \equiv b \pmod q \end{cases}$ (1) possui uma única solução

Se ... e somente se, $mdc(p, q) \mid a - b$

Caso essa solução exista, é única $mod(mmc(a, b))$

Prova: (→) Ida

Suponha que X seja uma solução para (1). Logo, $p \mid x - a$ e $p \mid x - b$

Assim, podemos escrever que $x - a = pk_1$ e $x - b = qk_2$ Sendo $k_1, k_2 \in \mathbb{N}$

Temos que: $a - b = qk_2 - pk_1$ (2)

Como podemos perceber, (2) é uma combinação linear de p e q. Isso é definitivamente verdade, mas pelo resultado anterior, sabemos que todas as combinações lineares de p e q são múltiplos do $mdc(p, q)$. Logo, isso significa que o mesmo é um múltiplo de $mdc(p, q)$