MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Neyman-Pearson Theorem). *Let $\mathcal{A}$ be a distinguisher, let $\alpha(A)$ be the ratio of false positives and let $\beta(\alpha)$ be the ratio of false negatives. Then we can define a weighted average $\delta(\mathcal{A}) = \lambda\alpha(\mathcal{A}) + (1-\lambda)\beta(\mathcal{A})$ for $\lambda \in [0, 1]$. Now consider two near-identical deterministic distinguishers which differ only on the input x_*:*

$$\forall x \neq x_* : \qquad \mathcal{A}_0(x) = \mathcal{A}_1(x) \enspace .$$

For clarity, let us assume $\mathcal{A}_0(x_*) = 0$ and $\mathcal{A}_1(x_*) = 1$. Establish under which conditions $\delta(\mathcal{A}_0) \geq \delta(\mathcal{A}_1)$ and conclude that describe the decision rule of a distinguisher that minimises δ. Let δ^*_λ be the attainable δ value for each λ. Each of these values δ^*_λ places a restriction on attainable $\alpha(\mathcal{A})$ and $\beta(\mathcal{A})$ values on $\alpha\beta$-plane. Sketch the corresponding border lines and explain why The Neyman-Pearson theorem is a direct consequence.