[PTKB] Kolokwium 2 - opracowanie

1 Zadanie 1.

Treść: Ile razy trzeba wykonać protokół uwierzytelniania Fiata-Shamira by prawdopodobieństwo oszustwa było mniejsze od 10^{-1000}?

Rozwiązanie: Prawdopodobieństwo udanego oszustwa po wykonaniu n eksperymentów wynosi $(\frac{1}{2})^n$. Rozwiązujemy równanie $(\frac{1}{2})^x = 10^{-1000}$.

$$\begin{aligned} (\tfrac{1}{2})^x &= 10^{-1000} \\ 2^x &= 10^{1000} \\ x &= \log_2 10^{1000} \\ x &= 1000 \log_2 10 \\ x &\simeq 3321.928 \end{aligned} \tag{1}$$

Wybieramy $\lceil x \rceil = 3322$.