Exercise # 1 (2 points)
You are trying to factor \( n = 642401 \). Suppose you discover that

\[ 516107^2 \equiv 7 \mod n \]

and that

\[ 187722^2 \equiv 2^2 \cdot 7 \mod n. \]

Can you factor \( n \)? (Hint: \( x^2 - y^2 = (x + y)(x - y) \)).

Exercise # 2 (2 points)
Find all irreducible polynomials over \( \mathbb{Z}_2 \) of degree 3 and 4. Verify that \( X^8 + X^4 + x^3 + X + 1 \) (i.e. the Rijndael polynomial) is irreducible.

Exercise # 3 (2 points)
Compute the entry in position \((9, 11)\) in the Rijndael S-box. Attention, we start labelling the rows and columns from 0, so position 9 is actually the 10-th row, for example.

Exercise # 4 (2 points)
Suppose you want to find a 200 digit prime. Since you are clever, and since you attended all lectures, you don’t even try numbers which are divisible by either 2, 3, or 5. Using the prime number theorem, how many randomly chosen 200-digit numbers (not divisible by 2, 3, 5) do you need to test on average until you find a prime?

Exercise # 5 (2 points)
Can you fill in the missing digit in

\[ 2203\_714 \]

to make that number divisible by 33?

due Monday, 11/28/05.

There will be no class Friday 11/18/05.