

MCS 425: Codes and Cryptography

Homework 3

Due in class, Friday September 21

- (1) Write code or pseudocode to compute $x^a \pmod n$ (write or print out code).
- (2) Write code or pseudocode to find x, y so that $xa + yb = \gcd(a, b)$ using the extended Euclidean algorithm (write or print out code).
- (3) Let p be prime. Show that $a^p \equiv a \pmod p$ for all a .
- (4) Find all solutions of $12x \equiv 28 \pmod{236}$.
- (5) Find all solutions of $12x \equiv 30 \pmod{236}$.
- (6) Find all solutions of $x^2 \equiv 1 \pmod{231}$.
- (7) Compute the last 2 digits of 421^{522} by hand.
- (8) Find the unique $x \pmod{630}$ so that $x \equiv 3 \pmod{14}$ and $x \equiv 20 \pmod{45}$.