Hardware Security
-- Modular Exponentiation

Cybersecurity Specialization

What Do We Expect to Learn?

- What is modular exponentiation?
- Why it is important in security?
- How it is computed?
- Are there any security vulnerabilities?

- Background
  - Integer multiplication
  - Decimal to binary conversion

What is Modular Exponentiation?

- Modular: finding the remainder
  - $7 \div 2 = 3$ with remainder 1.
  - $7 \equiv 1 \pmod 2$: 7 is congruent to 1 modulo 2
  - $a \equiv b \pmod n$: if $a-b = n*k$ for some integer k
- Modular exponentiation
  - $a^e \equiv ? \pmod n$
  - $2^4 \equiv 6 \pmod{10}$ because $2^4 = 16$
  - $34,987,317^{10,357,198} \equiv ? \pmod{510,926,533,897}$

Computing $a^e \pmod n$

- Exponentiation and modular
  - $a^e = b$
  - $b \pmod n$
- Iterative exponentiation and modular
  - If $x \equiv y \pmod n$, then $ax \equiv ay \pmod n$
  - Modular whenever larger than n
- How about $34,987,317^{10,357,198} \pmod{510,926,533,897}$?

Computing a^e (mod n)

- Exponentiation and modular
  - $a^e = b$
  - b (mod n)
- Iterative exponentiation and modular
  - If $x \equiv y \pmod{n}$, then $ax \equiv ay \pmod{n}$
  - Modular whenever larger than n
- Question for hardware designer: can we multiply less than e-1 times?