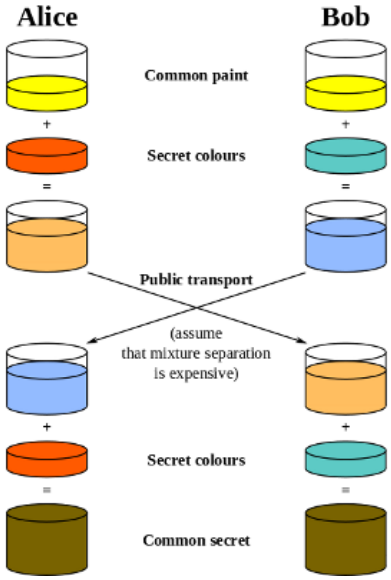
# MATH 480/580: Special Topics In Applied Math
# Introduction to Cryptography

Spring 2015 TR 7:00pm-8:15pm

## Topics:

- Early cryptosystems including shift and substitution ciphers
- Design of cryptosystems, public-key cryptosystems, the Diffie-Hellman, ElGamal, and RSA systems
- Combinatorial and probabilistic methods for attacking public-key cryptosystems.
- Mathematical topics include modular arithmetic, the Chinese Remainder Theorem, prime factorization, group theory, rings, polynomials, finite fields, primality testing, discrete logarithms, elliptic curves, P vs. NP, information theory
- DES and AES standards, digital signatures

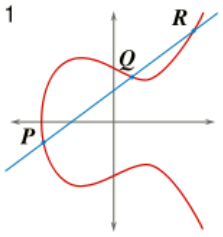



$$e : \mathcal{K} \times \mathcal{M} \to \mathcal{C} \qquad d : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

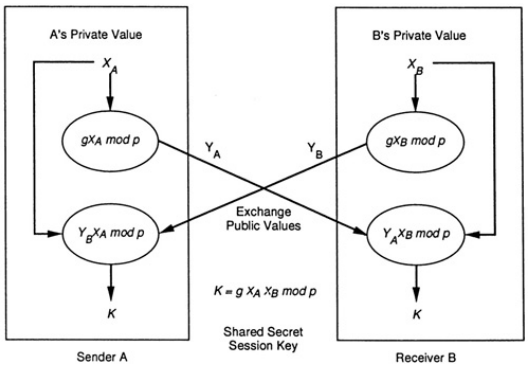
$$a^{p-1} \equiv 1 (\mod p)$$

## Prerequisites:

- MATH 207 (Discrete Structures I) or MATH 295 (Intro to Abstract Math)
- MATH 203 (Linear Algebra)
- Or permission of instructor




$$y^2 = x^3 + ax + b$$




Think you've got what it takes? Try to crack this:

**HWYGRBJFGSPYIIESIBHGBAAJU**

Contact Prof. Jason Howell (howelljs@cofc.edu) for more information.