Pries: 360 Mathematics of Information Security
Sample Final.

Warm-up:

1. Review the major topics we’ve covered: Euclidean algorithm, primes and factorization, \( \phi \) function, modular arithmetic, multiplicative inverses, Chinese remainder theorem, Fermat, Euler, dot products, binary numbers, primitive roots, order, discrete logs, linear recurrence relations, finite fields, error-correcting codes.

2. What is \( \phi(24) \) and what does it mean?

3. Find a number \( x \) so that \( 0 \leq x \leq 23 \) and \( x \equiv 9 \mod 24 \).

4. Use the table on page 137 of the handout to find \( 2^{23} \mod 37 \).

5. Decrypt Caesar’s shift message: KSSHPYGO!

Earlier Material:

1. For how many choices of \( a \) with \( 0 \leq a \leq 604 \) is the affine cipher \( x \to ax + b \mod 605 \) not 1-to-1?

2. Let \( a_1 = 3 \mod 13 \), \( a_2 = 2 \cdot 3 \mod 13 \), \( a_3 = 4 \cdot 3 \mod 13 \), \( a_4 = 8 \cdot 3 \mod 13 \), etc.
   What is the period of the sequence \( a_1, a_2, a_3, a_4, \ldots \)?

3. What are the last three digits of \( 6^{803} \)?

4. Use the table on page 137 of the handout to find all solutions to \( 4x^3 \equiv 13 \mod 37 \).

5. Use the table on page 137 of the handout to find a primitive root \( g \mod 37 \) (other than \( g = 2 \)) and to find the order of \( 25 \mod 37 \).

Recent Material:

1. Find a polynomial \( f(x) \in \mathbb{Z}/2[x] \) of degree 4 which factors mod 5 but does not have a root mod 5.

2. Find a polynomial in \( \mathbb{Z}/2[x] \) with degree smaller than 3 which is the same as \( f(x) = x^5 + x^3 + x \mod g(x) = x^3 + x + 1 \) (and mod 2).

3. Find the order of \( \beta \) in the finite field \( \mathbb{F}_8 \) with the relations \( \beta^3 + \beta + 1 = 0 \) and \( 2 = 0 \).

4. Find a basis for the ISBN code. In other words, find 9 codewords so that every possible ISBN codeword can be found by adding together scalar multiples of these 9.

5. Look at the linear code which is the set of vectors \((a_1, a_2, a_3, a_4, a_5)\) where each \( a_i \) is 0 or 1 and \( a_4 = a_2 + a_3 \mod 2 \) and \( a_5 = a_1 + a_2 \mod 2 \).
   A. What is the length \( n \)?
   B. What is the dimension \( k \)?
   C. What is the information rate?
   D. What is the distance \( d \) and the relative minimum distance?
E. How many errors can this code detect?

F. How many errors can this code correct?

Ideas and proofs:

1. Be able to briefly and clearly describe the following topics and their importance in cryptography: shift cipher, affine cipher, Vigenere cipher, substitution cipher, frequency analysis, diffusion, confusion, one-time pads, public key cryptosystem, RSA cryptosystem, El Gamal cryptosystem, signature scheme, hash function, DES and Rejdael.

2. Review encryption and decryption with the affine cipher, Vigenere cipher, RSA cryptosystem and El Gamal cryptosystem.

3. Find all primes of the form $p = n^2 - 1$ and explain why you’ve got them all.

4. If $p \equiv 3 \mod 4$, prove that $(p - 1)/2$ is odd. Include every detail!

5. Use the previous problem to show that $-1 = x^2 \mod p$ has no solution if $p$ is a prime and $p \equiv 3 \mod 4$. 