MATH 4175 Notes

Kevin Lee

December 10, 2012

August 27th

Affine Cipher $e(\alpha = 3\alpha + 5 \mod 26)$

$$\begin{array}{ccc} 1(A) & 8(H) & 8 = 3*1+5 \\ 2(B) & 11(K) & 11 = 3*2+5 \end{array}$$

$\forall x, \exists a : e(x) = ax + b \mod n,\ d(y) = a^{-1}(y-b) \mod n$
Here, $a = 3, b = 5, a^{-1} = 9$.

This is because $d(w) = 9 * 3 = 27 \equiv 1 \mod 26 = d(23) = 9(23-5) = 9*18 = 152 = 22 \mod 26 = V$
Affine cipher mod(n) must satisfy $e(x) = ax + b \mod n$, where a and n have no common divisor except 1

August 29th

Affine cipher example:

$$\begin{array}{cccccc} FMXVE & DKAPH & FERBN & DKRXR & SREFM & ORUDS \\ DKDVS & HVUFE & DKAPR & KDLYE & VLRHHRH & \end{array}$$

$e(x) = ax + b \mod n$, where $\gcd(a, n) = 1$
The # of these: if $n = 26$, ans = 12 (throw out even numbers and 13) * 26 = 312 (too many)
To solve, use frequency of letters:

$$\begin{array}{cc} R(8) & H(5) \\ D(7) & K(5) \\ ... & ... \end{array}$$

Let $e(E) = R = e(5) = 5a + b \mod 26 = 18 \mod 26$
Let $e(T) = D = e(20) = 20a + b \mod 26 = 4 \mod 26$

$$4 \mod 26 = 20a + b \mod 26 \tag{1}$$
$$18 \mod 26 = 5a + b \mod 26 \tag{2}$$

Subtracting (2) from (1) results in $(-14 \mod 26 = 15a \mod 26)$ or $(12 \mod 26 = 15a \mod 26)$
As $15^{-1} = 7, 7 * 15a \equiv 7 * 12 \mod 26 = 6$ which wont work because $\gcd(6, 26) \neq 1$

Instead of $e(T) = D$, Let $e(T) = K = 20a + b \mod 26 = 11 \mod 26$

$$11 \mod 26 = 20a + b \mod 26 \tag{3}$$
$$18 \mod 26 = 5a + b \mod 26 \tag{4}$$

Subtracting (4) from (3) results in $(-7 \mod 26 = 15a \mod 26)$ or $(19 \mod 26 = 15a \mod 26)$

$15^{-1} \mod 26 = 7$
7 comes from $(7 * 15 = 105 = 1 + 4 * 26 \equiv 1 \mod 26)$
This becomes $7 * 15a \equiv 7 * 19 \mod 26$
Since $7 * 15 = 1 \mod 26$, we have $a = 133 = 3 \mod 26$ and $e(x) = 3x + b$
We know that $5a + b = 18 \mod 26$, thus b is 3 and $e(x) = 3x + 3 \mod 26$

if $e(\alpha) = a\alpha + b \mod n$, then $d(\beta) =$ means solving for α in the congruence $a\alpha + b \equiv \beta \mod n$
$d(\beta) = \alpha^{-1}(\beta - b) = \alpha^{-1}(\beta - 3) = 9(\beta - 3) \mod 26 = 9\beta - 27 \mod 26 \equiv 9\beta - 1 \mod 26$

$e(5) = 18$, so d(18) = 5
$5 = a^{-1}(18 - 3) \mod 26$
$5 \equiv 9(15) \mod 26$

Decoded solution:

$$\begin{array}{cccccc} ALGOR & ITHMS & AREQU & ITEGE & NERAL & DEFIN \\ ITION & SOFAR & ITHME & TICPR & OCESSES & \end{array}$$

So the question is, how to find the inverse of a mod(n)?

1. Find the GCD of a and n (use euclidean algorithm)
   Euclid's observation: If $a = bq + r$, then $gcd(a, b) = gcd(b, r)$
2. From the GCD, calculate inverse

Ex. Find $GCD(118, 267)$, find $118^{-1} \mod 267$

$$267 = 2 * 118 + 31$$
$$118 = 3 * 31 + 25$$
$$31 = 1 * 25 + 6$$
$$25 = 4 * 6 + 1$$
$$6 = 6 * 1 + 0$$

The last non-zero remainder is the GCD (1)

Write out the quotients bottom to top

	4	1	3	2
1	4	4*1+1=5	5*3+4=19	19*2+5=43
+	-	+	-	+

1 = 25 - 4 * 6
1 = 25 - 4(31-1*25)
1 = -4 * 31 + 5 * 25
1 = -4 * 31 + 5 (118 - 3*31)
1 = 5 * 118 - 19 * 31
1 = 5 * 118 - 19 (267 - 2 * 118)
1 = -19*267 + 43*118 (43 is the inverse to 118!)

August 31st

Ex. Find

$$482 = 2 * 216 + 50$$
$$216 = 4 * 50 + 16$$
$$50 = 3 * 16 + 2$$
$$16 = 2 * 8 + 0$$

Thus, the GCD is 2

2 = 50 - 3 * 16
2 = 50 - 3(216 - 4 * 50)
2 = -3 * 216 + 13 * 50
2 = -3 * 216 + 13 (482 - 2 * 216)
2 = 13 * 482 - 29 * 216

	3	4	2
1	3	13	29
+	-	+	-

Take the last two with the signs to get 2 = 13 * 482 - 29 * 216
As a congruence of 482, we have $2 \equiv -29 * 216 \mod 482$, thus 216 is not invertible.
Suppose $\exists d : 216d \equiv 1 \mod 482$ but this is not possible.

Eulers (sounds like boilers)
For n is a positive integer, $\phi(n) = |a| 1 \leq a \leq n and \gcd(a, n) = 1|$
$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(p) = p - 1, \phi(p^2) = p^2 - p, \phi(p^r) = p^r - p^{r-1}$
$\phi(pq) = pq - q - p + 1 = (p - 1)(q - 1)$
If $(a, b) = 1, \phi(ab) = \phi(a)\phi(b)$

September 3rd

1. Kerkhoffs Law - When designing a crypto system that is hard to break, you must always assume that the other party knows everything about the crypto system. The key determines the secrecy.
2. Shannon's Law of Diffusion - Changing one plain text character affects several cipher text characters and vice versa.
3. Shannon's Law of Confusion - The cipher text does not relate to the key in a simple way.

Polyalphabetic ciphers
Vigenère cipher
The key is a string of length n called the keyword.
Kasiski Test - Look for trigraphs or longer that repeat

September 5th

Vigenère cipher

- Determine monoalphabetic vs polyalphabetic
- Two ways to determine the key length
  1. Kasiski Test
  2. IC - The index of coincidence
     The IC of a string of characters is the probability that two randomly chosen characters from the string are the same
     If the alphabet has characters $c_1, c_2, c_3, ..., c_r$, then the answer to P_r (picking 2 c_1's) + P_r(picking 2 c_2's) + ... $= \sum_{i=i}^{r} P_r(2\ c_i\text{'s})$ where $P_r(2 \text{ char's } c_i) = \dfrac{c_i}{\#chars} * \dfrac{\#c_i - 1}{\#chars - 1}$ where # chars = number of characters in the string
     Let f_i = # of instances of c_i, $ANS \begin{pmatrix} f_i \\ 2 \end{pmatrix} = \dfrac{f_i(f_i - 1)}{2}$
     Thus for a string of length R, IC = $\sum_{i=1}^{r} \frac{f_i}{R} * \frac{f_i - 1}{R - 1}$ where r is the alphabet size
     If $f_1 = f_2 = ... = f_r$, then R = string length = r * f. Then IC = $\sum_{i=1}^{r} \frac{f(f-1)}{rf(rf-1)} = \frac{1}{r} \sum_{i=1}^{r} \frac{f-1}{rf-1} = \frac{1}{r} \frac{r(f-1)}{rf-1} = \frac{f-1}{rf-1} = \frac{1}{r}$
     For a language on r characters with $p_i = P_r(\text{char} = c_i)$, IC(language) $= \sum_{i=1}^{r} p_i^2$
     This IC(english) ≈ 0.066

September 7th

Hill Cipher (first cipher to have qualities of confusion and diffusion):
Idea of Hill cipher: [A=0,B=1,...,Z=25]

1. Pick an interger n>1
2. Construct M, and n x n matrix mod(26)
3. Break plaintext into strings of length n
4. Encrypt: If $x = (x_1, x_2, ..., x_n) \leftarrow$ row vector
   then $e(x) \equiv x * M \mod 26$
5. Decrypt: If $y = x * M \mod 26$ ... M must be invertible.
   Then $y * M^{-1} \equiv (x * M) * M^{-1} \equiv x(M * M^{-1}) \equiv x * I \equiv x \mod 26$
   So M is invertible if and only if the determinate of M is an invertible integer mod 26
   Note: $I = M * M^{-1} \rightarrow 1 = det(I) = det(M) * det(M^{-1}) \mod 26$
   Therefore must have gcd(det(M), 26) = 1

Ex. GRINCH $\rightarrow$ (6 17)(8 13)(2 7)

$$M = \begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix}^{GR} : \begin{pmatrix} 6 & 17 \end{pmatrix} \begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix} \equiv \begin{pmatrix} 25 & 24 \end{pmatrix} \mod 26$$

$$IN \begin{pmatrix} 8 & 13 \end{pmatrix} \begin{pmatrix} . & . \\ . & . \end{pmatrix} \equiv \begin{pmatrix} 17 & 20 \end{pmatrix} \mod 26$$

$$CH \begin{pmatrix} 2 & 7 \end{pmatrix} \begin{pmatrix} . & . \\ . & . \end{pmatrix} \equiv \begin{pmatrix} 9 & 24 \end{pmatrix} \mod 26$$

Therefore GRINCH $\rightarrow$ ZYRUJY

Ex. HOWAREYOUTODAY
CT: ZESENIUSPLJVEU
Let M = $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$
HO = (7 14)M $\equiv$ (25 22) mod 26
WA = (22 0)M $\equiv$ (18 4) mod 26
$\rightarrow \begin{pmatrix} 7 & 14 \\ 22 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 25 & 22 \\ 18 & 4 \end{pmatrix} \mod 26$
det$\begin{pmatrix} 7 & 14 \\ 22 & 0 \end{pmatrix} = 7 * 0 - 22 * 14 \equiv 4 \mod 26$ (Wont work)
5th pair: (u t) = (20 19)
(20 19)M $\equiv$ (15 11) mod 26
$\rightarrow$ 1st and 5th pair = $\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} \mod 26$
$\therefore \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix}$

September 10th

Stream ciphers - An algorithm is used to generate a stream of key bits that are xored with the plaintext to encrypt it. Decrypting is done by xoring the encrypted values with the same stream of key bits.

Linear Recurrences:

1. Pick a positive integer m
2. Initialize: pick
   (a) Constants $c_0, c_1, c_2, ..., c_{m-1}$
   (b) an m-length binary string $(k_i, ..., k_m)$

3. Define z_i [the output of the recurrence] by $z_i = k_i$ for $1 \leq i \leq m$ and $z_i + m = c_0 z_i + c_1 z_{i+1} + ... + c_{m-1} z_{i+m-1}$ for $i \geq 1$. This is called a linear recursion recurrence

Ex. M = 4, $z_{i+4} = z_i + z_{i+1} \mod 2$
Every two bits gets exored together and appended to the end of the stream. The bits that are used are then incremented by one and the process continues. The bits starts to repeat every 15 bits.
Ex. M = 7, You get 127 bits
Ex. M = 31, You get > 2 billion bits

Ex. M = 11, A = 01, T = 1, H = 0000 (Morris code) Plaintext: 110110000 Key: 011010111 Ciphertext: 101100111

Linear Feedback Shift Register (LFSRs):
$|z_i|z_{i+1}|z_{i+2}|z_{i+3}| = |1|1|0|1|$ (Initial Fill)
$|z_i|z_{i+1}|$ gets xored, shifted into the rightmost register. The output from the left gets xored with the message to encrypt/decrypt.

If the degree [length of initial fill] is m, the period in a divisor (before repeats) is $2^m - 1$

September 12th

LFSR

1. A linear recurrence mod 2
2. Produces a keystream
3. Super fast!

Cryptoanalysis of LFSR:

Ex. Bitstream = 011010111...
Recurrence: $z_{m+i} \equiv c_0 z_i + c_1 z_{i+1} + ... + c_{m-1} z_{i+m-1} \mod 2$
Test: $m = 2, z = z_{2+i} \equiv c_0 z_i + c_1 z_{1+i} \mod 2$
$z_1 = 0, z_2 = 1, z_3 = 1 = c_0 z_1 + c_1 z_2 = c_0 \times 0 + c_1 \times 1 \rightarrow c_1 = 1$
No solution for c_0, $c_1 = 1$
$0 \equiv z_4 \equiv c_0 z_2 + c_1 z_3 \equiv c_0 \times 1 + c_1 \times 1 \rightarrow c_0 = 1$
$1 = z_5 = z_3 + z_4 = 1 + 0 = 1$
$0 = z_6 = z_4 + z_5 = 0 + 1 = 1$ Thus m $\neq$ 2

Test: $m = 3, c_0 z_1 + c_1 z_2 + c_2 z_3 = z_4$
$c_0 z_2 + c_1 z_3 + c_2 z_4 = z_5$
$c_0 z_3 + c_1 z_4 + c_2 z_5 = z_6$

Rewriten as matrix:

$$\begin{bmatrix} z_1 & z_2 & z_3 \\ z_2 & z_3 & z_4 \\ z_3 & z_4 & z_5 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} z_4 \\ z_5 \\ z_6 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Thus m $\neq$ 3 as the matrix is not invertible

If m = 4, the matrix is invertible

The main LFSR theorem: Let $M = \begin{bmatrix} z_1 & ... & z_m \\ z_2 & ... & z_{m+1} \\ z_m & ... & z_{2m-1} \end{bmatrix}$ with $z_1, ..., z_{2m-1}$ bits

1. If $z_1, ..., z_{2m-1}$, satisfies linear recurrence of order < m, then $\det(M) \equiv 0 \mod z$
2. OTOH if $z_1, ..., z_{2m-1}$ satisfies a linear recursion of order m and $\det M \equiv 0 \mod z$, then $z_1, ..., z_{2m-1}$ satisfies a linear recursion of order < m

In summary: M is invertible mod z $\Leftrightarrow$ $z_1, ..., z_{2m-1}$ satisfies no linear recurrence of length < m

Another example: suppose $z_i, ...$ satisfies $z_{i+3} = c_0 z_i + c_1 z_{i+1} + c_2 z_{i+2} \mod 2$

$$\begin{bmatrix} z_1 & z_2 & z_3 & z_4 & = & c_0z_1 + c_1z_2 + c_2z_3 \\ z_2 & z_3 & z_4 & z_5 & = & c_0z_2 + c_1z_3 + c_2z_4 \\ z_3 & z_4 & z_5 & z_6 & = & c_0z_3 + c_1z_4 + c_2z_5 \\ z_4 & z_5 & z_6 & z_7 & = & c_0z_4 + c_1z_5 + c_2z_6 \end{bmatrix}$$

Last column: $\begin{pmatrix} z_4 \\ z_5 \\ z_6 \\ z_7 \end{pmatrix} - c_0 \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} - c_1 \begin{pmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{pmatrix} - c_2 \begin{pmatrix} z_3 \\ z_4 \\ z_5 \\ z_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$\therefore$ the determinate of the above matrix is 0 as the last column is a linear combination of the first 3 columns

September 19th

Permutation on a set χ is a map $alpha : \chi \to X$ that is one to one and onto.

Two notations:

1. The 2 row form: $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$
2. The cycle decomposition: $\alpha = (13)(24)(31)(42)(55)$
   $\beta = (12453)$
   $\alpha \circ \beta = (13)(24)(31)(42)(55) \circ (12453) = (145)(2)(3)$

September 21st

Review: A,B,C,D,E,F are the first six enigma permutations for a given daily setting. The permutations D*A E*B and F*C are independent of the plaintext.
Signature of a setting = cycle structure of D*A, E*B, F*C
Permutation: 1-1 map of a set onto itself
Permutations are invertible
Two row permutation: Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 9 & 3 & 10 & 4 & 1 & 6 & 5 & 8 & 2 \end{pmatrix}$
$\pi = (2\ 9\ 8\ 5\ 4\ 10)(1\ 7\ 6)(3)$ (3 disjoint cycles)
$\sigma = (1\ 5\ 3\ 6\ 2)(4\ 7\ 8)(9\ 10)$
$\pi\sigma = (2\ 9\ 8\ 4\ 3\ 10)(1\ 76)(3)(1\ 5\ 3\ 6\ 2)(4\ 7\ 8)(9\ 10) = (4\ 6\ 9\ 2\ 7\ 5\ 3\ 1)(10\ 8)$
*Read from right to left
$\sigma\pi = (1\ 8\ 3\ 6\ 5\ 7\ 2\ 10)(4\ 9)$
Q: Do $\alpha\beta$ have the same cycle structure?
Inverses: Given n $f : X \to Y$ is 1-1 and onto, define $f^{-1} : Y \to X$ by $f^{-1}(r) = s$, where $f(s) = r$
Let $\gamma = \begin{pmatrix} 1 & 2 & ... & n \\ \gamma(1) & \gamma(2) & ... & \gamma(n) \end{pmatrix}$. Then $\gamma^{-1} = \begin{pmatrix} \gamma(1) & \gamma(2) & ... & \gamma(n) \\ 1 & 2 & ... & n \end{pmatrix}$
Conjugacy: Let α and β be permutations. Then $\alpha\beta\alpha^{-1}$ is called the α conjugate of β
$\beta = (3\ 5\ 1)(2\ 4)$, $\alpha = (1)(2\ 3\ 4\ 5)$
$\alpha\beta\alpha^{-1} = (1)(2\ 3\ 4\ 5)(3\ 5\ 1)(2\ 4)(5\ 4\ 3\ 2)(1)$=(1 4 2)(3 5)
Note: same cycle structure of β
Theorem: If α and β are permutations, then β and $\alpha\beta\alpha^{-1}$ have the same cycle structure.
Proof: We begin with a lennma.
If α and β are permuations, and β maps i to j, then $\alpha\beta\alpha^{-1}$ maps $\alpha(i)$ to $\alpha(j)$
Proof 1) $\alpha\beta\alpha^{-1}(\alpha(i)) = \alpha(\beta(\alpha^{-1}(\alpha(i)))) = \alpha(\beta(i)) = \alpha(j)$
Proof of theorem: Suppose $(a_1, a_2, ..., a_r)$ in a cycle of β, Then $\alpha\beta\alpha^{-1}$ takes $\alpha(a_1)$ to $\alpha(a_2)$, thus $\alpha\beta\alpha^{-1}$ in short $(a_1, a_2, ..., a_r)$ is a cycle of $\alpha\beta\alpha^{-1}$

The signature theorem: The signature of an enigma setting is independent of the plugboard.
Proof: ...

September 24th

Rejewshes

The shape of $D \circ A$ (its cycle structure) is independent of the plug board. If $A = S \circ \alpha \circ S$ and $D = S \circ \delta \circ S$ α is first setting without the plugboard, because S is its own inverse, we have $D \circ A = S \circ \delta \circ S \circ S \circ \alpha \circ S = S \circ (\delta \circ \alpha) \circ S = S \circ (\delta \circ \alpha) \circ S^{-1}$.

Theorem: Let α and β be permutations on 1,...,2n that are each a product of n disjoint 2-cycles. Then every cycle length in the cycle decomposition of $\beta \circ \alpha$ occurs an even number of times.

Ex. n = 4, # of perms = 4! = 24
Of this type: 1-1: (1)(2)(3)(4) = identity = 1 2-2: (12)(34)—(13)(24)—(14)(23) = 3 $\exists$ 4 such – Proof by induction: TPIBI on $n \geq 1$
Base case: n = 2, $\alpha = (12) = \beta$, $\beta\alpha = (1)(2)$
Th. Let n be an int > 1 and spse them is true for all k, $1 \leq k < n$. Finish. Let α and β be so in the statement of theorem.

Ex. $\alpha = (1\ 5)(2\ 7)(3\ 10)(4\ 9)(8\ 6)$
$\beta = (1\ 4)(7\ 10)(2\ 5)(8\ 3)(9\ 6)$
$\beta \circ \alpha = (1\ 2\ 10\ 8\ 9)(7\ 5\ 4\ 6\ 3)$

If we know that α and β are perms, and β sends i to j then $\alpha = \sigma\beta\sigma^{-1}$ sends $\sigma(i)$ to $\sigma(j)$.
ie. if $(a_1, a_2, ..., a_r)$ is a cycle of β, then $(\sigma(a_1), \sigma(a_2), ..., \sigma(a_r))$ is a cycle of $\alpha = \sigma\beta\sigma^{-1}$. Also if α and β have the same cycle type, then they are conjugates.

ex. $\beta = (1\ 3\ 5)(2\ 4)$
$\alpha = (2\ 5\ 3)(1\ 4)$
For any σ, we have $\sigma\beta\sigma^{-1} = (\sigma(1)\sigma(3)\sigma(5))(\sigma(2)\sigma(4)) = (2\ 5\ 3)(1\ 4)$
$\sigma(1) = 2, \sigma(3) = 5, \sigma(5) = 3, \sigma(2) = 1, \sigma(4) = 4$
$\sigma = (1\ 2)(3\ 5)(4)$
$\sigma\beta\sigma^{-1} = (1\ 2)(3\ 5)(4)(1\ 3\ 5)(2\ 4)(4)(3\ 5)(1\ 2) = (1\ 4)(2\ 5\ 3) = \alpha$

September 26th

$\sigma = (1\ 7\ 4)(5\ 8\ 9\ 2)(6\ 3)$ and $\tau\sigma\tau^{-1} = (5\ 6\ 3)(1\ 4\ 2\ 7)(8\ 9)$
If σ sends i to j, then $\tau\sigma\tau^{-1}$ sends $\tau(i)$ to $\tau(j)$
$(\tau(1) = 5,\ \tau(7) = 6,\ \tau(4) = 3)(\tau(5) = 1,\ \tau(8) = 4,\ \tau(9) = 2,\ \tau(2) = 7)(\tau(6) = 8,\ \tau(3) = 9)$
This results in $\tau = (1\ 5)(7\ 6\ 8\ 4\ 3\ 9\ 2)$
To find another possible value of τ, map τ to another value in the same cycle

Vernam Cipher (one time pad)

Eve gets to look at come ciphertext. What can she learn about the key?
Security:

- Computational - The ciphertext has no information on the key
- Provable - Can the key be verified to be correct
- Unconditional -

X is an experiment [aka random variable] with outcomes in some finite set $\mathbb{X}$
An event is a subset of the $\mathbb{X}$.
If x and y are outcomes, write $Pr(X) = x$ or $Pr(x)$ to mean (# successes/# trials).
$Pr(x, y)$ = probability that both x and y happen.
Mutual exclusivity: $Pr(x, y) = Pr(x)Pr(y)$
Independent and mutual exclusivity are not the same!

September 28th

Review for Exam 1:

Classical cryptosystems: Shift, Affine, Monoalphabetic Substitution, Polyalphabetic Substitution, Vigenere, Hill (Block), Linear Feedback Shift Register (Stream), Enigma

Mathematica topics: Congruences, Modular Arithmetic, Solving Linear Equations (ax + by = d in integers), GCD and Euclid's Alg, Extended GCD, Inversion (mod n), Matrix Inversion, Permutations, Conjugary, Eulerϕ function

Cryptoanalytics: Frequency Analysis, Mono/Di/Trigraphs, Kasiski Test (Viginare), Index of Coincidence, Finding Linear Recursions from a Bit Stream

October 3rd

Entropy - Let $\mathbb{X}$ be an experiment also known as a random variable, with outcome probabilities $p_1, ..., p_n$. H is a function that satisfies four properties.

1. For all $p_1, ..., p_n$ with $p_i \geq 0$ and $p_1 + ... + p_n = 1$, $H(p_1, ..., p_n)$ is a non-negative real number.
2. H is contiguous in each variable.
3. $H(\frac{1}{n}, ..., \frac{1}{n}) < H(\frac{1}{n+1}, ..., \frac{1}{n+1})$ thus n terms $< n+1$ terms.
   $H(\frac{1}{2}, \frac{1}{2}) < H(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$
4. If $0 < g < 1$, then $H(p_1, ..., p_i, qp_i, (1-q)p_i, p_{i+1}, ..., p_n) = H(p_1, ...p_i, ...p_n) + p_i H(q, 1-q)$
   Ex 1. x_1 = 'odd', x_2 = 'even', y_1 = '2', y_2 = '4 or 6' - a fair die.
   $H(\frac{1}{2}, \frac{1}{2})$
   $\{x_1, y_1, y_2\} \leftarrow H(\frac{1}{2}, \frac{1}{6}, \frac{1}{3})$ by (4)
   $H(\frac{1}{2}, \frac{1}{6}, \frac{1}{3}) = H(\frac{1}{2}, \frac{1}{2}) + \frac{1}{2} H(\frac{1}{3}, \frac{2}{5})$

What's H?
$H(\frac{1}{2}, \frac{1}{2})$ vs $H(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$
$H(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) : H(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}) = \frac{1}{2} H(\frac{1}{2}, \frac{1}{2}) + H(\frac{1}{2}, \frac{1}{2})$
$H(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) = H(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}) + \frac{1}{2} H(\frac{1}{2}, \frac{1}{2})$
$H(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) = H(\frac{1}{2}, \frac{1}{2}) + \frac{1}{2} H(\frac{1}{2}, \frac{1}{2}) + \frac{1}{2} H(\frac{1}{2}, \frac{1}{2})$
So $H(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) = 2H(\frac{1}{2}, \frac{1}{2})$
$H(\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}) = 3H(\frac{1}{2}, \frac{1}{2})$
$H(\frac{1}{2n}, ..., \frac{1}{2n}) = nH(\frac{1}{2}, \frac{1}{2})$
$H(\frac{1}{3n}, ..., \frac{1}{3n}) = nH(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$

Define $A(k) = H(\frac{1}{k}, ..., \frac{1}{k})$
$A(3n) = nA(3)$
$A(6) = A(2*3) = 2A(3) = A(3*2) = 3A(2)$
$A(6) = A(3) + A(3)$
$A(15) = A(5) + A(5) + A(5)$

Thml: If $H(X)$ satisfies prop's (1-4), for all X, then if $x_1, ..., x_n$ are outcomes with probabilities $p_1, ..., p_n$, then $H(p_1, ..., p_n) = -\lambda \sum_{i=1}^{n} p_i \log(p_i)$ where $p_i \neq 0$ for some positive constant λ.

October 5th

Def. Let $\mathbb{X}$ be an experiment with outcomes in a set (also called $\mathbb{X}$) and associated prob distribution. Then $H(\mathbb{X}) = -\sum_{x \in \mathbb{X}} Pr(x) \log_2(Pr(x)), Pr(x) > 0$. $H(\mathbb{X})$ is the expected value of $-log_2(Pr(x))$ But $\lim_{x \to 0} x \log_b(x) = 0$
What is the expected # of guesses needed to determine a particular #, about which you only know its range - S'?
Example S' = {0,1,2,3,4,5,6,7}

```
Q: Is n $>$ 3?
    Yes (1) - Is n $>$ 5?
        Yes (1) - Is n $>$ 6?
            Yes (1) - Answer is 7 (111)
```

```
            No (0) - Answer is 6 (110)
        No (0) - Is n $>$ 4?
            Yes (1) - Answer is 5 (101)
            No (0) - Answer is 4 (100)
    No (0) - Is n $>$ 1?
        Yes (1) - Is n $>$ 2?
            Yes (1) - Answer is 3 (011)
            No (0) - Answer is 2 (010)
        No (0) - is n $>$ 0?
            Yes (1) - Answer is 1 (001)
            No (0) - Answer is 0 (000)
```

Let $x \in \{0, 1, 2, ..., 7\}$, and let $Pr(x) = \frac{1}{8}$
Then $E = -\sum_{x=0}^{7} Pr(x)\log_2(Pr(x)) = -\sum_{x=0}^{7} \frac{1}{8}\log_2\frac{1}{8} = -8(\frac{1}{8})\log_2(\frac{1}{8}) = -\log_2(2^{-3}) = -(-3)\log_2(2) = 3$

What is the expected # of guesses needed to determine the exact number of heads in the following experiment: we flip two fair (distinguishable) coins.
$\Pr(0 \text{ heads}) = \frac{1}{4}$, $\Pr(1 \text{ heads}) = \frac{1}{2}$, $\Pr(2 \text{ heads}) = \frac{1}{4}$
Are they the same?

```
Q: Are they the same?
    Yes (1/2) - Is there a head?
        Yes - Answer is 2 heads
        No -  Answer is 0 heads
    No (1/2) - Answer is 1 head
```

Answer $= \frac{3}{2}$
$Pr(0)\log_2(Pr(0)) + Pr(1)\log_2(Pr(1)) + Pr(2)\log_2(Pr(2)) = \frac{1}{4}\log_2(\frac{1}{4}) + \frac{1}{2}\log_2(\frac{1}{2}) + \frac{1}{4}\log_2(\frac{1}{4}) = \frac{1}{4}\log_2(4) + \frac{1}{2}\log_2(2) + \frac{1}{4}\log_2(4) = \frac{2}{4} + \frac{1}{2} + \frac{2}{4} = \frac{3}{2}$

October 8th

PSet6 Problem 3:
$H(X) = H(\frac{1}{2}, \frac{1}{2}) + \frac{1}{2}H(\frac{1}{2^8}, ..., \frac{1}{2^8}) + \frac{1}{2}H(\frac{1}{2^{32}-2^8}, ..., \frac{1}{2^{32}-2^8})$
where $H(\frac{1}{n}, ..., \frac{1}{n}) = \sum_{x=1}^{n} \Pr(x)\log_2(Pr(x)) = -n * \frac{1}{n} * \log(\frac{1}{n}) = \log_2 n$

Eve gets to see some ciphertext. How much does she know about the plaintext than when she did not observe the ciphertext?
Conditional Entropy: Given two experiments X and Y, define $H(Y|X) := \sum_{X}(\Pr(X = x)H(Y|X = x)) = \sum_{x\in X}\Pr(x)\sum_{y\in Y}(\Pr(y|x)\log_2\Pr(y|x))$. Recall $\Pr(y|x) = \dfrac{\Pr(y,x)}{\Pr(x)}$. So $\Pr(y|x)\Pr(x) = \Pr(y,x)$. Thus $H(Y|X) = -\sum_{x\in X y\in Y}\Pr(x)\Pr(y|x)\log_2\Pr(y|x) = -\sum_{x\in X y\in Y}\Pr(y,x)\log_2\Pr(y|x)$

A cryptosystem has perfect secrecy provided $H(P|C) = H(P)$.

October 10th

Huffman Encoding - Begin with an experiment X with outcomes and probabilities.
0.5 a $\leftrightarrow$ 00
0.3 b $\leftrightarrow$ 01
0.1 c $\leftrightarrow$ 10
0.1 d $\leftrightarrow$ 11

Write down outcomes together with their probabilities.
Pick the two outcomes with the smallest probabilities, assign 1 to one of them and 0 to the other.
c $\rightarrow$ 1, d $\rightarrow$ 0
Combine the two event outcomes into one, with the probability = sum of the two previous.

c/d $\to$ 1, b $\to$ 0
b/c/d $\to$ 0, a $\to$ 1
Repeat till only one outcome.
Encode each outcome by writing the bits in reverse order from final outcome to initial outcome.
a $\to$ 1, b $\to$ 00, c $\to$ 011, d$\to$ 010
L = expected length of bit (encoding) string for the outcomes = avg. # of bits = 0.5(1)+0.3(2)+0.1(3)+0.1(3) = 1.7 < 2
Entropy $H(X) = -(0.5\log_2 0.5 + 0.3\log_2 0.3 + 0.2\log_2 0.1) \approx 1.685$
L is bounded on the lower end by the entropy and upper end by entropy + 1.

The entropy of English:
Random characters (26) = $\log_2(26) \approx 4.7$
Random character w/ space = $log_2(27) \approx 4.75$
Monographic distribution ≈ 4.18
Digraphs = $H(x|x_{-1}) \approx 3.56$
Trigraphs = $H(x|x_{-1_2}) \approx 3.3$
If L^N = probability distribution of N graphs, then H(English) = $\lim_{N\to\infty} \frac{H(L^N)}{N}$

October 15th

Coding vs crypto - error (detect/correct) codes - sending message over noisy networks (crypto sends over nosy networks)
Detecting errors - codeword = message + check
Possibilities:
1. duplicate message – (1011) + (1011) = (10111011)
2. parity check – (1011) + xor(1011) = (1011) + (1) (append a bit to make # of 1s even)
Correcting errors - harder than detecting
1. Triplication - message bit = x, code word = xxx
An (n,k) code is a code with codewords of length n and messages of length k

October 17th

Practical error correction
Terminology
Code = strings from an alphabet (all of the same length)
An (n,k) code is a code in which the code words have length n and there are k message characters.

The data rate per bit for an (n,k) code C [over {0,1}] with w codewords in all - is defined by $r = \frac{log_2(w)}{n}$
For an (n,n) code, the data rate $d = \frac{log_2(2^n)}{n} = 1$ (no error correction)
Triplication code: a (3,1) code - M = 0, send 000, M = 1, send 111. n = 3, w = 2 so $r = \frac{log_2(2)}{3} = \frac{1}{3}$
The 2x2 code: the code word is a string of 8 bits $(x_1, x_2, ..., x_8)$ where bits 1, 2, 4, and 5 are message bits, bit 3 = 1 xor 2, bit 6 = 4 xor 5. The bits received $(y_1, y_2, ..., y_3)$ are put into an array $\begin{array}{cc|c} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \\ \hline y_7 & y_8 & \end{array}$

A = $y_1 + y_2 + y_3$
B = $y_4 + y_5 + y_6$
C = $y_1 + y_4 + y_7$
D = $y_2 + y_5 + y_8$

Wrong bits (pairs)	Error bit
A,C	y_1
B,D	y_5
A,D	y_2
B,C	y_4

Wrong bits (single)	A	B	C	D
	y_3	y_6	y_7	y_8

data rate: n = 8, k = 4, w = 2^4, therefore $r = \frac{log_2(2^4)}{8} = \frac{1}{2}$

Efficient encoding: code = block of 7 bits x_1 to x_7 where x_3, x_5, x_6, x_7 are message bits.
Choose x_4 to make $\alpha = x_4 + x_5 + x_6 + x_7 = 0$ (mod 2).
Choose x_2 to make $\beta = x_2 + x_3 + x_6 + x_7 = 0$ (mod 2)
Choose x_1 to make $\gamma = x_1 + x_3 + x_5 + x_7 = 0$ (mod 2).

Blocks received, compute α, β, γ.
Read $\alpha\beta\gamma$ as a binary integer j.
j = subscript such that x_j is incorrect if $j = 1, ..., 7$.
If $j = 0$, then there are no errors.

Let $(x_1x_2x_3x_4x_5x_6x_7)$ = 1111101, $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = 110$

Thus error in bit 6.
β = 010, 011, 110, 111 (second bit is 1)
α = 110, 101, 110, 111 (first bit is 1)

October 19th

Hamming distance - defection and connection
The Hamming (7,4) code - another look
The Hadamard Code - Let x,y be strings of the same length. H(x,y), the hamming distance between x and y is defined to be the number of positions at which x and y differ.
Ex. let x = 1001100 and y = 0101011. H(x,y) = 5

Binary: weight of x = # of 1s = # of non-0 bits
If x and y are bit strings, then H(x,y) = weight of xored strings

Theorem: Let C be a code with minimum distance d between code words. Then
a) C can detect up to d-1 errors
b) C can correct up to (d-1)/2 errors

Hamming Code: 4 message bits, 3 parity bits - send 7 bits
Hadamard Code: 6 message bits, 26 parity bits - send 32 bits
data rate = $\log_2(2^6)/32 = 6/32$

October 22nd

Hadamard Code (32,6) code, length = 32 bits, message = 6 bits.
More generally, (2^n,n+1) codes
(32,6) corrects up to 7 errors.
(16,5) corrects up to 3 errors.
(2^n,n+1) corrects up to $2^{n-2} - 1$ errors.

For the (16,5) code: messages are the 32 integers with a binary representation of no more than 5 bits.

Two matrices of interest: a generating matrix G (produces the codeword), a parity check matrix P. G is a 4x16 matrix, with the columns numbered j = 0,...,15. The jth column is the 4 bit representation of j. That is, if $j = 8j_3 + 4j_2 + 2j_1 + j_0$, then the jth column of G is $\begin{pmatrix} j_3 \\ j_2 \\ j_1 \\ j_0 \end{pmatrix}$ Thus G = $\begin{bmatrix} 0 & 0 & 0 & ... & 1 & 1 & 1 \\ 0 & 0 & 0 & ... & 1 & 1 & 1 \\ 0 & 0 & 1 & ... & 0 & 1 & 1 \\ 0 & 1 & 0 & ... & 1 & 0 & 1 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 1 & 0 & ... & 13 & 14 & 15 \end{bmatrix}$

let $x = x_4 + x_3 + x_2 + x_1 + x_0$ be a 5 bit message word.
To encode x:

1. Form $x^x = (x_3, x_2, x_1, x_0)$
2. Form the 16 long vector $y = x^* * G \mod 2 = (y_1, ..., y_15)$
3. For $1 < i < 16$, set $z_i = (-1)^{y_i}$

   For 26 = 11010, x^* = (1,0,1,0)
   $x^* * G = (0, 0, 1, 1, ...)$

4. Set $z = (z_1, ...z_16)$ if $x_4 = 0$ (ie. if $0 \leq x \leq 15$) $= (-z_1, ..., -z_16)$ if $x_4 = 1$ (ie. if $16 \leq x \leq 31$) where z is the encoding of x

To decode, form the parity check matrix P, a 16x16 (-1,1) matrix whose jth row is the encoding of j, for $0 \leq j \leq 15$.
Let w be a 16-long vector of 1s and -1s. Form w * P.

# of errors	Range for all dot products but 1	Range for the ''right'' one	Can determine correct message?
0	0	16 or -16	Yes
1	-2 to 2	14 to 16 or -14 to -16	Yes
2	-4 to 4	12 to 16 or -12 to -16	Yes
3	-6 to 6	10 to 16 or -10 to -16	Yes
4	-8 to 8	8 to 16 or -8 to -16	No

Can detect up to 7 errors but correct up to 3 errors.

Constructing parity check matrix for Hadamard codes

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} : H_1 * H_1^t = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2I_2$$

$$H_2 = \begin{pmatrix} H_1 & H_1 \\ H_1 & H_1 \end{pmatrix} : H_2 * H_2^t = 4I_4$$

$$H_3 = \begin{pmatrix} H_2 & H_2 \\ H_2 & H_2 \end{pmatrix}_{8x8} : ...$$

$$H_4 = \begin{pmatrix} H_3 & H_3 \\ H_3 & H_3 \end{pmatrix} : ... = P$$

1001100 is a codeword in (7,4)
Each codeword is 1 away from seven non-codewords.

October 24th

A q-ary code is a code that uses a set of q characters
Def 1. Let C be a code [ie, a set of vectors of fixed length] over a character set of q characters. Let w be a code word and $t \in \{0, 1, ...\}$
The sphere $B(w, t)$ of radius t about the word w is defined by $B(w, t) = \{\text{strings } s | H(w, s) \leq t\}$
Prop 1. Let C be a code of length n and let w be a codeword. Then $|B(w, t)| = 1 + \begin{pmatrix} n \\ 1 \end{pmatrix} (q - 1) + \begin{pmatrix} n \\ 2 \end{pmatrix} (q - 1)^2 + ... + \begin{pmatrix} n \\ t \end{pmatrix} (q - 1)^t$.

$B(w,t)$ contains 1 string s: $H(s,w) = 0 \to s = w$
# of strings with $H(s,w) = 1 = \begin{pmatrix} n \\ 1 \end{pmatrix} * (q-1)$.
# of strings with $H(s,w) = 2$? $\exists \begin{pmatrix} n \\ 2 \end{pmatrix}$ pair of positions to alter, each having $(q-1)^2$ ways of altering each pair.

Th. (Sphere Packing Bound/Hamming Bound) - If C is a q-ary code of length n, and minimum distance d, and if t is a positive integer such that d $\geq$ 2t+1, then the number M of code words satisfies $M \leq \frac{q^n}{\sum_{j=0}^{t} \begin{pmatrix} n \\ j \end{pmatrix} (q-1)^j}$.

Proof. Because d $\geq$ 2t+1, t $\leq \llcorner (d-1)/2 \lrcorner$, and so this code can correct as many as t errors.
If w_1 and w_2 are distinct codewords, then $B(w_1,t)$ and $B(w_2,t)$ do not overlap. Therefore if there are M codewords, then there are at least $M * \sum_{j=0}^{t} \begin{pmatrix} n \\ j \end{pmatrix} (q-1)^j$ strings in the code. But the number of strings in the space $= q^n$. Therefore $M * \sum_{j=0}^{t} \begin{pmatrix} n \\ j \end{pmatrix} (q-1)^j \leq q^n$.

Def 1. If a q-ary code of length n with M codewords satisfies the Hamming bound with equality, that code is called perfect.

Claim: The Hamming (7,4) code is perfect.
Proof: We have q=2, n= 7, and d = 3. Each sphere about a code word of radius $\llcorner (d-1)/2 \lrcorner = 1$ has $\sum_{j=0}^{1} \begin{pmatrix} 7 \\ j \end{pmatrix} (2-1)^j = 1 + 7 = 8$ strings. $16 = M \leq \frac{q^n}{\sum} = \frac{2^7}{1+7} = 2^4 = 16$.

The (15,11) Hamming code is also perfect. The parity bits are 1,2,4,8.
1 = 1 + 3 + ... + 15 == 0
2 = 2 + 3 + 6 + 7 + ... == 0
4 = 4 + 5 + 6 + 7 + 12 + 13 + 14 + 15 == 0
8 = 8 + 9 + 10 + ... + 15 == 0
n = 15, d = 3, thus $M * \sum_{j=0}^{1} \begin{pmatrix} 15 \\ j \end{pmatrix} (2-1)^j \leq 2^{15}$ Thus $M \leq \frac{2^15}{1+15} = 2^{15-4} = 2^{11}$.

October 29th

PSet9 3a) Binary perfect 2-error correcting code of length n.
# of code words: $M * \sum_{j=0}^{t} \binom{n}{j} (q-1)^j = q^n$
q = 2, t = 2, we have $M(1 + n + \frac{n(n-1)}{2}) = 2^n$
Therefore $1 + n + \frac{n(n-1)}{2}) = 2^n$ is a power of 2, say 2^k. Then $\frac{n^2-n}{2} + n + 1 = 2^k \Rightarrow n^2 + n + 2 = 2^{k+1}$
$n^2 + n + (2 - 2^{k+1}) = 0$ (quadratic equation). So $n = \frac{1}{2}(-1 + \sqrt{1^2 - 4(1)(2-2^{k+1})}) = \frac{1}{2}(-1 + \sqrt{-7 + 2^{k+3}})$.
Therefore $2^{k+3} - 7$ is a square.

SPN - substitution permutation network - a crypto system that is broken up into units and run through a substitution box (s-box) then a permutation.
Our network: PT is 16 bits = four 4-bit strings. Key (K) is 32 bits = eight 4-bit strings. The 4-bit strings are the blocks.
Round: from previous round, you have a 16 bit string on hand which is derived somehow from the PT.
Round j: string on hand is called $w^{j-1}[j = 1, w^0 = PT]$ Take $w^{j-1} \oplus K^j$ and call this u^j [K^j is a "round key" of 16 bits, derived from the 32 bit key..]

Substitution: Take u^j and run it through the s-boxes. Call the result v^j.

Permutation: Take v^j and

1. Write it into a 4x4 array of bits, one row at a time.
2. Read it out by columns. Call this w^j.

3. Take $w^j \oplus K^{j+1} = u^{j+1}$

Exceptions: First round: $x = \text{PT}$, $w^0 = x = \text{PT}$, then $u^1 = w^0 \oplus K^1$
Last round: do not perform the permutation.

```
             PT
             \xor K
------------------
Round 1      S
             P
             \xor K
------------------
Round 2      S
             P
             \xor K
------------------
Round 3      S
             P
             \xor K
------------------
Round 4      S
             \xor K
```

Sequence of events for encryption:
K,S,P,K,S,P,K,S,P,K,S,K

Sequence of events for decryption:
K,S,**K,P**,S,**K,P**,S,**K,P**,S,K
The above pairs is equivalent

$$\text{abc def ghi} \rightarrow \begin{matrix} a & b & c \\ d & e & f \\ g & h & i \end{matrix} \rightarrow \text{adg beh cfi} \rightarrow \begin{matrix} a & d & g \\ b & e & h \\ c & f & i \end{matrix} \rightarrow \text{abc def ghi}$$

Key = 32 bits = $D_1D_2D_3D_4D_5D_6D_7D_8$ where D_i is a block of 4 bits.
$K^1 = D_1D_2D_3D_4$
$K^2 = D_2D_3D_4D_5$
$K^3 = D_3D_4D_5D_6$
$K^4 = D_4D_5D_6D_7$
$K^5 = D_5D_6D_7D_8$

Think of a 4-bit block as a hexadecimal number from 0-F.
Each s-box looks like this permutation: (0,E)(1,4,2,D,9,A,6,B,C,5,F,7,8,3)
Ex. 0110 1011 0010 1110 (4 blocks) = 6 B 2 E $\rightarrow$ B C D 0 (after permutation) = 1011 1100 1101 0000

$$B_1 + \text{Perm: } \begin{matrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{matrix} \Rightarrow 1110\ 0110\ 1000\ 1010 \text{ (columns)}$$

October 31st

16-bit PT, 32-bit Key K
PT $\oplus K^1$

```
--- Round 1 ---
S-Boxes
Bit Permutation
\xor K^2
---------------
```

```
--- Round 2 ---
S-Boxes
Bit Permutation
\xor K^3
---------------
--- Round 3 ---
S-Boxes
Bit Permutation
\xor K^4
---------------
--- Round 4 ---
S-Boxes
\xor K^5 = CT
---------------
```

S-box:
0 1 2 3 4 5 6 7 8 9 A B C D E F
E 4 D 1 2 F B 8 3 A 6 C 5 9 0 7

Bit permutation: $x_1 x_2 ... x_1 6$
Write this by columns in a 4x4 array and read it out by rows.

$K = B_1 B_2 B_3 B_4 ... B_8$
$K^1 = B_1 B_2 B_3 B_4$
$K^2 = B_2 B_3 B_4 B_5$
$K^3 = B_3 B_4 B_5 B_6$
$K^4 = B_4 B_5 B_6 B_7$
$K^5 = B_5 B_6 B_7 B_8$

Ex. PT = B A 5 6, K = 7 9 E 1 C D 3 4
K^1 = 7 9 E 1
etc..
Decryption uses S-box derived from old S-box.
BitPerm " " " BitPerm $\oplus$ K, key derived from round key S.

New S-box = S^{-1}, the inverse substitution of the original.
Given a, with b = bit permutation of a P(a), and c = $K^i \oplus$ b.
Want to write this: start with C, do a bit perm P'(C), P' related to P. Follow that with an xor with L^i, related to K^i.

November 2nd

Encrypt: PT $\rightarrow K^1 \oplus PT = a$
Round 1: $a \rightarrow S^1(a) = b, b \rightarrow P(b) = c, c \rightarrow K^2 \oplus c = d$
Round 2: $d \rightarrow S^1(d) = e, e \rightarrow P(e) = f, f \rightarrow K^2 \oplus f = g$
Last round: $S, \oplus$

Decrypt:
Specific to one round:
$e \rightarrow S^{-1}(e) = d$
$d \rightarrow P^*(d) = c^*$
$c^* \rightarrow L^4 \oplus c^* = b$
so $P^*(d) \oplus L^4 = b$.
$\therefore P(b) = P(P^*(d) \oplus L^4), P(b) \oplus K^4 = P(P^*(d) \oplus L^4) \oplus K^4 = d$
What if $P(x \oplus y) = P(x) \oplus P(y)$? Then $d = P(P^*(d)) \oplus P(L^4) \oplus K^4$.
Let $P^* = P^{-1}$, the inverse of P and $P(L^4) = K^4$ ie. $L^4 = P^{-1}(K^4)$, then $b = P^{-1}(d) \oplus L^4$

$\bar{x} = (x_1, x_2, ... x_n) \leftrightarrow x_1, x_2, ... x_n$ (bit string)

Ex. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$

$\pi(x_1, x_2, x_3, x_4, x_5) = (x_4, x_3, x_5, x_1, x_2)$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} x_4 \\ x_3 \\ x_5 \\ x_1 \\ x_2 \end{pmatrix}$$

If M is an n x m matrix and $\bar{x}$, $\bar{y}$ are n-dimensional vectors, then we know that M$(\bar{x} \oplus \bar{y})$ = M$(\bar{x}) \oplus$ M$(\bar{y})$

Decrypt: $L^j = P^{-1}(K^j)$, $S^* = S^{-1}$, $P^* = P^{-1}$

CT $\rightarrow$ CT $\oplus L^5 = w^5$, $L^j = P^{-1}(K^j)$

$\rightarrow S^{-1} \rightarrow P^{-1}$ (=P, for the one in the book) $\rightarrow \oplus L^4 = w^4$

$w^4 \rightarrow S^{-1} \rightarrow P^{-1} \rightarrow \oplus L^3 = w^3$ (Round 2)

$w^3 \rightarrow S^{-1} \rightarrow P^{-1} \rightarrow \oplus L^2 = w^2$ (Round 3)

$w^2 \rightarrow S^{-1} \rightarrow \oplus L^1 =$ PT (Round 4)

November 5th

Crypto-analysis for the block cipher:

$P(x \oplus y) = P(x) \oplus P(y)$ is linear, easily invertible.

Def: The bias of a function with outcomes {0,1} is defined by $\varepsilon : Pr(\mathbb{X} = 0) - \frac{1}{2}$.

Look for inputs $x_{i1}, ..., x_{iu}$ and outputs $y_{j1}, ..., y_{jv}$ for which $x_{i1} \oplus ... \oplus x_{iu} \oplus y_{j1} \oplus ... \oplus y_{jv} = 0$ has a bias that's "big".

Let $\mathbb{X}_1, \mathbb{X}_2$ be random variables with outcomes in {0,1}. Set p_i = Pr$(\mathbb{X}_i = 0)$; then Pr$(\mathbb{X}_i = 1) = 1 - p_i$.

What is Pr$(\mathbb{X}_1 \oplus \mathbb{X}_2 = 0)$?

Pr$(\mathbb{X}_1 = 0, \mathbb{X}_2 = 0)$ + Pr$(\mathbb{X}_1 = 1, \mathbb{X}_2 = 1)$ $= P_1 * P_2 + (1 - P_1)(1 - P_2)$. Substitute $P_i = \frac{1}{2} + \varepsilon_i = (\frac{1}{2}+\varepsilon_1)(\frac{1}{2}+\varepsilon_2)+(\frac{1}{2}-\varepsilon_1)(\frac{1}{2}-\varepsilon_2) = \frac{1}{4}+\varepsilon_1\varepsilon_2+\frac{1}{2}(\varepsilon_1+\varepsilon_2)+\frac{1}{4}+\varepsilon_1\varepsilon_2-\frac{1}{2}(\varepsilon_1+\varepsilon_2) = \frac{1}{2}+2\varepsilon_1\varepsilon_2 = \Pr(X_1 \oplus X_2 = 0)$.

$\therefore$ Bias $(\varepsilon_{1,2})$ for $X_1 \oplus X_2 = 2\varepsilon_1\varepsilon_2$.

$\Pr(X_1 \oplus X_2 \oplus X_3 = 0) = \Pr((X_1 \oplus X_2) \oplus X_3 = 0) = \frac{1}{2} + 2(\varepsilon_1, \varepsilon_2)(\varepsilon_3) = \frac{1}{2} + 2 * 2\varepsilon_1\varepsilon_2\varepsilon_3$.

$\therefore \varepsilon_{1,2,3} = 2^2\varepsilon_1\varepsilon_2\varepsilon_3$

The Piling-up Lennma: If $x_1, ..., x_n$ are independent r.vs with biases $\varepsilon_1, ..., \varepsilon_n$, then the biases of $x_1 \oplus ... \oplus x_n$ is equal to $2^{n-1}\varepsilon_1, ..., \varepsilon_n$.

November 7th

$\Pr(X_1 \oplus X_3 \oplus X_4 \oplus Y_2 = 0) = \frac{12}{16}$, bias $= \frac{1}{4}$

Deduce a statement of the form $P_{i1} \oplus P_{i2} \oplus ... \oplus P_{ir} \oplus C_{j1} \oplus ... \oplus C_{js} \oplus K_{l1} \oplus ... \oplus K_{lt} = 0$ where $K_{l1} \oplus ... \oplus K_{lt}$ is fixed.

$u_{i,j}$ = jth bit of the input to the ith round of the S-box.

$v_{i,j}$ = jth bit of the output of the ith round of the S-box.

ith round S_i = 4 nibble $S_{i,1}, S_{i,2}, S_{i,3}, S_{i,4}$

We know that $v_{1,6} \oplus u_{1,5} \oplus u_{1,7} \oplus u_{1,8} = 0$ with p $= \frac{12}{16}, \sum = \frac{1}{4}$

$v_{1,6} \oplus (P_5 \oplus K_{1,5}) \oplus (\oplus) \oplus (\oplus) = 0$ with p $= \frac{3}{4}, \sum = \frac{1}{4}$

November 9th

Midterm 2
Begins with permutations
Know how the enigma machine works
Entropy
Huffman encoding
Up through definition of bias

AES - 128bit input string, key ranges from 128, 256, 512 bits with 10, 12, and 14 rounds.

Fields with 2^n elements.

November 12th

$\mathbb{F}_4 = \{0, 1, f, f+1 \text{ where } y + y = 0 \text{ for all } y \text{ and } f^2 = f + 1\}$

K is a field. (K,+) is an abelian group, (K-{0},*) is an abelian group.
$\mathbb{F}_4 \subseteq \mathbb{F}_8$?
Lagranges Theorem. If G, H are finite groups and H $\subseteq$ G, then $|H|$ divides $|G|$.
$(\mathbb{F}_4, +)$ has 4 elements
$(\mathbb{F}_8, +)$ has 8 elements
$(\mathbb{F}_4 - \{0\}, *)$ has 3 elements
$(\mathbb{F}_8 - \{0\}, *)$ has 7 elements
Thus $\mathbb{F}_4 \not\subseteq \mathbb{F}_8$

$\mathbb{F}_8 = \{0, 1, g, g+1, g^2, g^2+1, g^2+g, g^2+g+1\}$
$\mathbb{F}_8 = \{a_0 + a_1 g + a_2 g^2 \text{ where } a_i \in \{0,1\}, g^3 = g + 1\}$

f satisfies the polynomial equation in $x^2 + x + 1 = 0$
g satisfies the polynomial equation in $x^3 + x + 1 = 0$

$\mathbb{F}_2[x] = \{a_0 + a_1 x + ... + a_n x^n \text{ where } a_i \in \{0,1\}, n \in \{0, 1, ...\}\}$

Over $\mathbb{R}, x^2 + x + 1 = (x+a)(x+b) \to a + b = 1, ab = 1, x = \frac{-1 \pm \sqrt{1^2 - 4(1)(1)}}{2} = \frac{-1 \pm \sqrt{-3}}{2}$
$\mathbb{F}_4 = \mathbb{F}_2[x] \mod (x^2 + x + 1)$

The AES field $= \mathbb{F}_2[x] \mod (x^8 + x^4 + x^3 + x + 1)$

November 26th

Finite Fields
For p a prime, begin with $\mathbb{Z}_p[x] = \{a_0 + a_1 x + ... + a_n x^n | a_i \in \mathbb{F}_p, n = 0, 1, 2, ...\}$
If (n,p) = 1, then Euclidean GCD algorithm $\Rightarrow \exists a, b, \in \mathbb{Z} : an + bp = 1$
Read this as congruence mod p, we have $an \equiv 1 \mod p$

Def: let $a(x) \in \mathbb{Z}_p[x]$
Then $a(x)$ is irreducible provided

1. $\deg(a(x)) \geq 1$
2. if $a(x) = d(x)e(x)$, for $d(x), e(x) \in \mathbb{Z}_p[x]$, then either $d(x)$ or $e(x)$ is a constant $\neq 0$.

[ln $\mathbb{Z}_5[x], 2x + 1 = 2(x + 3)$]

Let $f(x)$ be a non zero poly. Then $a(x) \equiv b(x) \mod f(x)$ provided $a(x) - b(x)$ is a multiple of $f(x)$. Division "works like" integer division. ie. Given $f(x), g(x)(f(x) \neq 0)$, both in $\mathbb{Z}_p[x], \exists$ unique $q(x), r(x) \in \mathbb{Z}_p[x] : g(x) = q(x)f(x) + r(x)$ with $\deg(r) < \deg(f)$ or $r \equiv 0$.

Example: find polynomial gcd $x^4 + 2x^3 + x + 1, x^3 + x + 1)$ over $\mathbb{Z}_3[x]$.
$x^4 + 2x^3 + x + 1/x^3 + x + 1 = x + 2$ re $-x^2 - 2x - 1$
$x^3 + x + 1/ - x^2 - 2x - 1 = -x + 2$ re $4x$
$-x^2 - 2x - 1/x = -x - 2$ re -1

To construct a field with p^r elements, where r > 1 and p is a prime:

1. Find an irreducible poly $f(x) \in \mathbb{F}_p[x]$ of degree r
2. The set $\{a_0 + a_1x + ... + a_{r-1}x^{r-1} | a_i \in \mathbb{F}_p\}$ is a field with p^r elements.
   Arithmetic is in $\mathbb{Z}_p[x] \mod f(x)$

Ex. A field with 27 elements. Look for a poly of degree 3 = r that is irreducible over $\mathbb{Z}_3[x]$.
$f(x) = x^3 + 2x + 1$ (irreducible)
$\mathbb{F}_33 = \{a_0 + a_1x + a_2x^2 | a_i \in \mathbb{Z}_3$ and $x^3 + 2x + 1 \equiv 0 \mod f(x), x^3 \equiv -2x - 1 \mod f(x) \equiv x - 1$ }
$(1 + x^2)(2 + x^2) = 2 + 2x^2 + x^2 + x^4 = 2 + x^4 = 2 + x^2 - x.(x^3 = x - 1, x^4 = x^2 - x)$
$\therefore (1 + x^2)(2 + x^2) = (2 - x + x^2)$

To find $(a_0 + a_1x + a_2x^2)^{-1}$, do poly GCD extended on $(a_0 + a_1x + a_2x^2, x^3 + 2x + 1)$.
$1 = a(x)(2 + x^2) + b(x)(x^3 + 2 + 1)$

November 28th

AES
PT → Add Key → [Byte Sub → Shift Rows → Mix Columns → Add Key] → Byte Sub → Shift Rows → Add Key → CT
Run through the round [ ] 9 times with a new key each time.
Key = 128 bits

Bytes (block of 8 bits) have two identities:

1. They're bit strings of length 8
2. They're elements of a 256-eleemnt field $\mathbb{F}_{2^8}$

$\mathbb{F}_{2^8} = \mathbb{Z}_2[x] \mod (x^8 + x^4 + x^3 + x + 1)$ (irreducible)
The byte $a_7a_6a_5a_4a_3a_2a_1a_0$ corresponds to the field element $a_7x^7 + a_6x^6 + ...a_1x + a_0 \in \mathbb{F}_{2^8}$
PT = 128 long bit-string - read it as 16 byte. Load these bytes into a 4x4 matrix down the columns.
Thus $b_0b_1...b_Eb_F$ becomes $\begin{bmatrix} b_0 & b_4 & b_8 & b_C \\ b_1 & b_5 & b_9 & b_D \\ b_2 & b_6 & b_A & b_E \\ b_3 & b_7 & b_B & b_F \end{bmatrix}$

Sub Bytes: fore each byte $y \in M$, define z by z = 0 if y = 0 or z = y^{-1} if y $\neq$ 0.
$*y^{-1}$ in $\mathbb{F}_{2^8}$
$y \rightarrow$ Byte to Field → [Inverse] → $z = y^{-1}$
$z \rightarrow$ Field to Vector → $(z_7, z_6, ...z_1, z_0)$

Multiply vector by matrix ... and add column vector.
y → $S * y^{-1} + cv \mod 2$ = Sub Bytes[y], S = large array, cv = constant vector

$f(x) = x^8 + x^4 + x^3 + x + 1$, to find $g(x)^{-1}$ in $\mathbb{Z}_2[x] \mod f(x)$, use Euclidean GCD algorithm to find $a(x), b(x)$ polynomial where $a(x) * f(x) + b(x) * g(x) = 1$. Thus $a(x) * 0 + b(x) * g(x) \equiv 1 \mod f(x)$. $b(x) * g(x) \equiv 1 \mod f(x)$.

November 30th

$$M = \begin{bmatrix} b_0 & b_4 & b_8 & b_C \\ b_1 & b_5 & b_9 & b_D \\ b_2 & b_6 & b_A & b_E \\ b_3 & b_7 & b_B & b_F \end{bmatrix}$$

Shift Rows: $\left(\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ ... & ... & ... & ... \\ ... & ... & ... & ... \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}\right) = \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ a_{2,2} & a_{2,3} & a_{3,3} & a_{2,1} \\ a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \end{bmatrix}$

Mix Columns: if S = state M + X

Mix Columns(S) = M * X, where M = $\begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix}$

M is a 4x4 matrix over $\mathbb{F}_{2^8}$

Byte To Field $(a_7a_6a_5a_4a_3a_2a_1a_0) = a_7x^7 + a_6x^6 + ... + a_1x + a_0 \in \mathbb{F}_{2^8}$

Field To Byte $(\sum_{i=1}^{7} b_ix^i = b_7b_6b_5b_4b_3b_2b_1b_0)$

$\mathbb{F}_{2^8} = \{a_0 + a_1x + ...a_7x^7 | a_i \in \{0,1\}$ and $x^8 + x^4 + x^3 + x + 1 = 0$ or $x^8 = x^4 + x^3 + x + 1\}$

Q: In $\mathbb{F}_{2^8}$, what is x^8?

A: Don't know, look at $\mathbb{F}_8$, where I might find a clue: $\mathbb{F}_8 = \{0, 1, b, 1+b, b^2, 1+b^2, b+b^2, 1+b+b^2\}$

$b^3 = b + 1$

$b^4 = b^2 + b$

$b^5 = b^3 + b^2 = b^2 + b + 1$

$b^6 = b^3 + b^2 + b = b + 1 + b^2 + b = b^2 + 1$

$b^7 = 1$

$\mathbb{F}_8 = \{0, b^7, b^5, b^6, b^4, b^5\}$

In $\mathbb{F}_{2^8}$, what's x?

$x^8 + x^4 + x^3 + x + 1 = 0$

$\therefore x^8 = -(x^4 + x^3 + x + 1) = x^4 + x^3 + x + 1$ (since 2 = 0)

$x^9 = x^5 + x^4 + x^2 + x$

$x^{10} = x^6 + x^5 + x^3 + x^2$

$x^{11} = x^7 + x^6 + x^4 + x^3$

$x^{12} = x^8 + x^7 + x^5 + x^4 = x^4 + x^3 + x + 1 + x^7 + x^5 + x^4 = x^7 + x^5 + x^3 + x + 1$

Q: In $\mathbb{F}_{2^8}$, what is x^8?

A: I think I believe the derivation that $x^8 = x^4 + x^3 + x + 1$

Round key generation: Add Round Key: $\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ ... & ... & ... & ... \\ ... & ... & ... & ... \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} \oplus$ current round key

Round keys are formed from the original key $K = k_0k_1...k_Ek_F$

Form $\begin{bmatrix} k_0 & k_4 & k_8 & k_C \\ k_1 & k_5 & k_9 & k_D \\ k_2 & k_6 & k_A & k_E \\ k_3 & k_7 & k_k & k_F \end{bmatrix} = [W(0), W(1), W(2), W(3)]$

O^{th} round key is $[W(0), W(1), W(2), W(3)]$.

To construct the jth round key $[W(4j), W(4j+1), W(4j+2), W(4j+3)]$ do the following: (given $W(0), ..., W(i-1)$)

$W(i) = W(i-1) \oplus W(i-4)$ if i is not a multiple of 4.

If $i \equiv 0 \pmod 4$, write $W(i-1) = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$;

Then $W(i) = W(i-4) \oplus \begin{bmatrix} SubBytes(b) \oplus x^{\frac{i-4}{4}} \\ SubBytes(c) \\ SubBytes(d) \\ SubBytes(a) \end{bmatrix}$

December 3rd

AES Decryption
SubBytes(SB) - ShiftRows(SR) - MixColumns(MC) - AddRoundKey(ARK)
Inverse of ARK is ARK (bytes are xored)
If $X = Y \oplus K$, then $X \oplus K = Y \oplus (K \oplus K) = Y$.

Inverse of MC(S) $= M * S$, where M $= \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} \in M_{4x4}(\mathbb{F}_{2^8})$:

Inverse of MC(S) is $M^{-1} * S$ where M^{-1} = inverse of M $= \begin{pmatrix} x^3+x^2+x & x^3+x+1 & x^3+x^2+1 & x^3+1 \\ x^3+1 & x^3+x^2+x & x^3+x+1 & x^3+x^2+1 \\ x^3+x^2+1 & x^3+1 & x^3+x^2+x & x^3+x+1 \\ x^3+x+1 & x^3+x^2+1 & x^3+1 & x^3+x^2+x \end{pmatrix}$
(circulant)

Inverse of SR: InvSR$(s_{i,j})_{i,j=0}^3 = \begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{13} & s_{10} & s_{11} & s_{12} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{31} & s_{32} & s_{33} & s_{30} \end{pmatrix}$

Inverse of SB:
SB(S): For each byte y, define $z := y^{-1} \in \mathbb{F}_{2^8}$ (if $y \neq 0$), $= 0$ if y = 0.

Then $w := \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \bullet \begin{pmatrix} z_0 \\ ... \\ z_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$. $M_s^{-1} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$ (circulant)

Then $y = z^{-1}$ if $z \neq 0$, $y = 0$ if $z = 0$

To decrypt: Let Rk(0),Rk(1),...,Rk(10) be the key schedule.
Begin with CT
Round 0: ARK(10),InvSR,InvSB
Round 1: ARK(9),InvMC,InvSR,InvSB
...
Round 9: ARK(1),InvMC,InvSR,InvSB
Round 10: ARK(0) $\rightarrow$ PT

December 5th

SDES
Message: 12 bits
Key: 9 bits = $k_1 ... k_9$
RKi = $k_i k_{i+1} ... k_{i+7}$ w/ wrap around
Two s-boxes S_1 and S_2, each is a 2x8 table
If $y_1 y_2 y_3 y_4$ is an input, y_1 addresses a row and $y_2 y_3 y_4$ addresses the column

Thus S =

	0	1	2	3	4	5	6	7
0								
1								

Ex. 1110 is the value in the second row, 6th column (output is a tribit)
Expander: $\text{Ex}(b_1b_2b_3b_4b_5b_6) = b_1b_2b_4b_3b_4b_3b_5b_6$

ith round: $p_1p_2...p_12 \to L_{i-1} = p_1...p_6, R_{i-1} = p_7...p_{12}$
$L_{i-1} \oplus f(R_{i-1}, K_i)$ to get R_i, same with other half
f function: $\text{Exp}(R_{i-1})$ (8bits) $\oplus K_i \to x_1x_2..x_8 \to S_1(x_1x_2x_3x_4)||S_2(x_5x_6x_7x_8) \to \oplus L_{i-1} \to R_i$

If $R_{i-1} = p_7..p_{12}$ then $\text{Exp}(R_{i-1}) = p_7p_8p_{10}p_9p_{10}p_9p_{11}p_{12} \oplus k_ik_{i+1}k_{i+2}k_{i+3}...k_{i+7}$ so $S_1(p_7p_8p_{10}p_9 \oplus k_ik_{i+1}k_{i+2}k_{i+3})||S_2(p_{10}p_9p_{11}p_{12} \oplus k_{i+4}k_{i+5}k_{i+6}k_{i+7}) = f(R_{i-1,K_i})$

December 10th

Review for Final Exam

Chapter 1 - Traditional Crypto [shift, affine, substitution [mono-alphabetic (cryptograms), poly-alphabetic (Vigenere)], stream cipher (LFSR), modular arithmetic, gcd algorithm, modular inversion, Kasiski test, IC, frequency analysis, LFSRs - solving for recursion, ENIGMA permutation [composition, conjugacy], details of the ENIGMA system, error correcting codes [encoding, decoding, Hamming distance, Hamming codes, Hadamard codes]

Chapter 2 - Shannon's information theory, entropy, Huffman encoding, one-time pads, probability, base theorem

Chapter 3 - Block ciphers, hill cipher, SPNs, Sbox, key schedule, AES [implementation, subbytes, shiftrows, mixcolumns], finite fields arithmetic, polynomial GCDs

In $\mathbb{F}_8 = \mathbb{Z}_2[x] \mod x^3+x+1$: $(x^2+x)(x^2+x+1) = x^4+x^3+x^2+x^3+x^2+x = x^4+x \equiv x^2 \mod x^3+x+1$