Christopher Seaman
Discrete Mathematics for Cryptographic Applications
Wednesday, October 24, 2007

MIDTERM

All work is my own.

1. There is a block cipher, F, such that $F(A+B) = F(A) + F(B)$, (where $+$ is XOR).

A known plaintext attack can reduce this encryption method to linear algebra. Let the block size be n and $\{e_1, ..., e_n\}$ the usual basis for $\mathbb{Z}_2^n$ under component-wise addition. Note that for $k_j \neq i$, $F(e_i) \neq F(e_{k_1}) + F(e_{k_2}) + ... + F(e_{k_t})$ because that would violate the linear independence of $\{e_1, ..., e_n\}$. It follows directly that $\{F(e_1), ..., F(e_n)\}$ are linearly independent, given the relation in the premise. We will define an $n \times n$ matrix using the column vectors $\begin{pmatrix} F(e_1) & ... & F(e_n) \end{pmatrix}$ in order, denoting $F(e_j)$ as the n-tuple $(e_{j,1}, e_{j,2}, ..., e_{j,n})$ with $e_{j,k} \in \mathbb{Z}_2$.

$$G = \begin{pmatrix} F(e_1) & ... & F(e_n) \end{pmatrix} = \begin{pmatrix} e_{1,1} & e_{2,1} & ... & e_{n,1} \\ e_{1,2} & e_{2,3} & ... & e_{n,2} \\ ... & ... & ... & ... \\ e_{1,n} & e_{2,n} & ... & e_{n,n} \end{pmatrix}$$

Right-multiplying the matrix G by a basis vector gives its encrypted form. Matrix multiplication is distributive so $G \cdot (v_1 + v_2) = (G \cdot v_1) + (G \cdot v_2)$. Also, any block may be expressed through the addition of a finite number of basis elements. Putting it all together (with secret message $m = e_{k_1} + e_{k_2} + ... + e_{k_t}$):

$$\begin{aligned} G \cdot m &= G \cdot (e_{k_1} + e_{k_2} + ... + e_{k_t}) \\ &= (G \cdot e_{k_1}) + (G \cdot e_{k_2}) + ... + (G \cdot e_{k_t}) \\ &= F(e_{k_1}) + F(e_{k_2}) + ... + F(e_{k_t}) \\ &= F(m) \end{aligned}$$

Cool! We can express the cipher as $G \cdot m = c$ for secret message m and ciphertext c. But we've also got that G is made up of n linearly independent columns, so G is invertible. Finally, $G^{-1} \cdot (G \cdot m) = G^{-1} \cdot c \Rightarrow m = G^{-1} \cdot c$ and the cipher is broken.

2. Sometimes order matters. Does it here? Prove/Disprove.

A. DES

Not commutative. You can think of the combined steps of the bit selection table and s-boxes as a member of $S_{2^{32}}$. Each DES encryption involves 16 of these which, unless specifically chosen from a commutative subgroup of $S_{2^{32}}$, will not be commute with another 16 group members (they're not chosen that way). So, not commutative. Also, by example (in hex):

Plaintext	1st DES Key	1st Ciphertext	2nd DES Key	Final Ciphertext
0000000000000000	0000000000000000	8ca64de9c1b123a7	1111111111111111	b9dab3ce1f2be617
0000000000000000	1111111111111111	82e13665b4624df5	0000000000000000	112822c5e83e0d02

B. Mono-alphabetic Substitution

Not commutative. By example, let substitution $m_1 = (ab)$ and $m_2 = (abc)$. This gives us:

$$\begin{aligned} m_1 \cdot m_2(c) &= m_1(a) = b \\ m_2 \cdot m_1(c) &= m_2(c) = a \end{aligned}$$

And $m_1 \cdot m_2 \neq m_2 \cdot m_1$. There are mono-alphabetic substitution subgroups that do commute, but they are the exception and not the rule. This is also obvious by noticing that the space of mono-alphabetic substitutions is isomorphic to S_{26}.

C. Vigenère

Commutative. Vigenère is a block cipher acting on text, it increments each letter by an amount defined by the corresponding position in the key. So each Vigenère key is a set of offsets by which the plaintext letters are rotated ("FIRE" increments by (5, 8, 17, 4)). As such we may consider the space of Vigenère ciphers of key length n to be members of the group $\mathbb{Z}_{26}^n$ under component-wise addition (applying "FIRE" = (5, 8, 17, 4) twice is the same as (10, 16, 8, 8) = "KQII"). Also note that concatenation of the key preserves the cipher ("FIREFIRE" is the same as "FIRE"). Vigenère ciphers of different length keys (n_1 and n_2 with least common multiple m) can act on each other in the group $\mathbb{Z}_{26}^m$. Thus, the question of commutativity boils down to whether addition is commutative in Z_{26}. It is.