MATH 587/CSCE 557 - SUMMARY OF CLASS, 1/16/07

After introducing myself and giving the course information (all of which can be found on the course webpage www.math.sc.edu/∼boston/587.html), I gave a list of topics to be covered, namely classical cryptography, attacks on it such as frequency analysis, entropy, linear feedback shift registers and pseudorandom sequences, (asymmetric) public-key cryptography (RSA), and (symmetric) private-key cryptography (DES, AES).

Cryptology = cryptography (code-making) + cryptanalysis (code-breaking).

Until about 1970, cryptographers were mostly government/military or amateur puzzle-solvers.

The Caesar Cipher:- To encrypt, shift the letters of the alphabet by 3, so $A \to D, B \to E, ...W \to Z$. What about X, Y, Z? Do it cyclically, so $X \to A, Y \to B, Z \to C$. To decrypt, shift back by 3 letters, the inverse operation, called decryption.

Shift Ciphers:- Can shift by any number to encrypt, not necessarily 3.

Classical Cryptosystems:- P, C, K denote the sets of plaintexts, ciphertexts, and keys respectively. For each k in K, there are two functions, encryption $e_k : P \to C$ and decryption $d_k : C \to P$ such that $d_k(e_k(x)) = x$ for all x in P. If $P = C$, call it the message space.

For our example, $P = \{A, B, C, ..., Z\} = C$ and $K = \{0, 1, 2, ..., 25\}$. Note that $e_k(x) = e_r(x)$ where $r = k \pmod{26}$, meaning the remainder on dividing k by 26, so we only really have 26 different keys. $e_k(x)$ is the kth letter after x and $d_k(x)$ is the kth letter before x, so $d_k(x) = e_{-k}(x) = e_{26-k}(x)$.

More compactly, identifying A with 0, B with 1, C with 2, ..., Z with 25, we have $P = C = K = \{0, 1, 2, ..., 25\}$ (= $\mathbf{Z}_{26}$, see below) and $e_k(x) = x + k \pmod{26}, d_k(x) = x - k \pmod{26}$.

Block Ciphers:- P and C consist of blocks of letters of some given length and a string of blocks $x = x_1x_2...x_n$ is encrypted to $e_k(x_1)e_k(x_2)...e_k(x_n)$ (i.e. juxtapose).

Stream Ciphers:- The encryption of a symbol also depends on its position (and possibly earlier symbols).

Modular Arithmetic:- Integers $\pmod{N}$ are $\mathbf{Z}_N := \{0, 1, 2, ..., N-1\}$.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX