THE UNIVERSITY OF SYDNEY
MATH3024 ELEMENTARY CRYPTOGRAPHY AND PROTOCOLS

Semester 1 **Exercises for Week 6** 2004

Three-time pads

1. Given $\Delta_1 = XY \ominus ZW$ and $\Delta_2 = XY \ominus QR$, the matrix of relative probabilities $P(XY|\Delta_1, \Delta_2)$ can be computed with this function.

```
function RelativeDifferentialProbabilities(D1,D2,PT)
    // Given 2-character strings D1 and D2 representing
    // XY-ZW and XY-QR, return the 26x26 matrix of
    // probabilities, (P(XY)P(ZW)P(QR)), scaled to a
    // probability function on the set {A,..,Z}^2.
    // PT is a sample plaintext for use in determining
    // the 2-character frequency distribution of English.
    assert #D1 eq 2 and #D2 eq 2;
    AZ := {@ CodeToString(64+i) : i in [1..26] @};
    r1 := Index(AZ,D1[1]); s1 := Index(AZ,D1[2]);
    r2 := Index(AZ,D2[1]); s2 := Index(AZ,D2[2]);
    FDD := RealField()!0;
    DD2 := MatrixAlgebra(RealField(),26)!0;
    F2D := DigraphFrequencyDistribution(PT);
    for i1, j1 in [1..26] do
        i2 := ((i1-r1) mod 26) + 1;
        j2 := ((j1-s1) mod 26) + 1;
        i3 := ((i1-r2) mod 26) + 1;
        j3 := ((j1-s2) mod 26) + 1;
        F3 := F2D[i1,j1] * F2D[i2,j2] * F2D[i3,j3];
        DD2[i1,j1] +:= F3;
        FDD +:= F3;
    end for;
    return (1/FDD)*DD2;
end function;
```

Apply this function to find the plaintexts PT_1, PT_2, and PT_3, where

$$\Delta_1 = PT_1 \ominus PT_2 = \texttt{AHXCOYFBAMKUE}$$
$$\Delta_2 = PT_1 \ominus PT_3 = \texttt{XHXRGEUHPRAHN}$$

You may use *blackcat.txt* as the sample plaintext.

Modes of Operation

Block ciphers can be applied to longer ciphertexts using one of various *modes of operation*. We assume that the input is plaintext $M = M_1M_2\ldots$, the block enciphering map for given key K is E_K, and the output is $C = C_1C_2\ldots$. The following gives a summary of the major modes of operation.

Electronic Codebook Mode. For a fixed key K, the output ciphertext is given by $C_j = E_K(M_j)$ with output $C_1C_2\ldots$.

Ciphertext Block Chaining Mode. For input key K, and initialization vector C_0, the output ciphertext is given by $C_j = E_K(C_{j-1} \oplus M_j)$, with output $C_0C_1C_2\ldots$.

Ciphertext Feedback Mode. Given plaintext $M_1M_2\ldots$ in r-bit blocks, a key K, an n-bit cipher E_K, and an n-bit initialization vector $I = I_1$, the ciphertext is computed as:

$$C_j = M_j \oplus L_r(E_K(I_j))$$
$$I_{j+1} = R_{n-r}(I_j) \,||\, C_j$$

where R_{n-r} and L_r are the operators which take the right-most $n-r$ bits and the left-most r bits, respectively, and $||$ is concatenation.

Output Feedback Mode. Given plaintext $M_1M_2\ldots$ in r-bit blocks, a key K, an n-bit cipher E_K, and an n-bit initialization vector $I = I_0$, the ciphertext is computed as:

$$I_j = E_K(I_{j-1})$$
$$C_j = M_j \oplus L_r(I_j),$$

where L_r is the operator which takes the left-most r bits.

2. What mode of operation has been used in the assignment and in class up to this point? Why?

3. Let E_K be the 4-bit cipher defined by:

$$E_K(M) = (X_1 + X_3, X_2 + X_4, X_2 + X_3, X_1 + X_4)$$

where $X = X_1X_2X_3X_4 = K \oplus M$. Encipher the message M given by

$$11010110111001110010010001001000,$$

using the key $K = 1011$, in (i) ECB mode, in (ii) CBC mode with initialization vector 1001, and in (iii) CFB mode with initialization vector 1001 and $r = 1$.

4. How many steps are required for error recovery from a ciphertext transmission error in ECB and CBC modes?

5. If $n = 64$ and $r = 8$, how many steps in CFB mode does it take to recover from an error in a ciphertext block? What about in OFB mode?