Problem Set 2

Due: February 27

1. Decipher the following ciphertext, which was created using the Vigenere cipher. As usual, the line breaks have no significance. Briefly describe how you obtain your answer.

```
JSJTEWXQVRFLOSNJRXCFXJSYTQZMNZ
FYILLGKRXNGJVVRMIMWGOAIBWOPSJY
BSXVVRDQGYNROJWGQKBTTOLSPHBYBW
TNOVSCFXJSAJQKRQKGTLMRVVRFHLIN
CCJUFLQIEQULITVRBUKGTCHHBWHKBG
MYKRQKVSNZIFFLHLWIMPRIBWAGBGKI
JACFQTHCRGSFFHVINPBBMSRFKUJHZI
TSNHBWHVVRQUKXQTGMYKQCZYIUJOLI
ANJWVVFRJMZIEFBZWZIFEHNYLPAHBX
NWEFMUNMTVGOGMUFHVVRSLSMUSQMCE
WGZSXFGANMNSXDSQYRIIMXVVRDQWVG
FHSHARICAYBWTNOVSBSVTMVSALLGOA
YYDSRSNSXLLGOAYYDSRSZTPWHNWXJJ
ZEPHBRMARVVRXHGACBQHCJGNSQFHVA
JSRQYVEPRGMYVVADBBXWVDZRBUTSWH
GMYEMPHUJWGPFABTHDMIVGFHVXJSVW
VJICHUXGGOGRCFFWPAWAYBWGQZQFMA
JVVRDVMVPSQBCLLUCZJCFRGFSNLWEP
RGMYOSNJRXNOMUHRIUFHVIESYVEPRY
JUHXKBNXCDIPQRXOULVVNYNZIAGRJG
WHQTNSILLGFJTLDHGBGNLWXJSLRINI
FRBBHLLGJNQFWCCBQYOJRGRNSXESXS
QKUJSWHBSNZIRZNNHMRVWYYBWCYSEJ
NZIUANQFWWVCSKCYYTSFNHLLCHQNGO
LKHRSYKWCBQYBWRVVRDXAWCDCJUJIF
```

2. Stinson, problem 2.28, p.58 (Stinson discusses the Autokey Cipher on pp.37-38.)

3.

i. In each round, the DES function f takes as input a 32-bit string R_{i-1} (the right half of the current block), and a 48-bit string K_i (the round key). Prove that for any R_{i-1}, K_i,

$$f(R'_{i-1}, K'_i) = f(R_{i-1}, K_i),$$

where for any bitstring X, X' denotes the bitwise complement of X.

ii. Prove that if

$$DES(K, X) = C$$

(that is, applying DES to plaintext X with key K produces ciphertext C), then

$$DES(K', X') = C'.$$

[**Hint**: Use part (i)]

(This problem is a restatement of Stinson's problem 4.3 on p.132. I have broken the problem into two steps.)

4. In section 4.5.2, Stinson observes that the security of DES is based in part on the *non-linearity* of the S-Boxes. To say that an S-Box S_i is *linear* is to say that for any bitstrings x_1 and x_2 of length 6,

$$S_i(x_1 \oplus x_2) = S_i(x_1) \oplus S_i(x_2).$$

Thus to say that the S-Boxes are non-linear is to say that, for each S-Box, there are pairs of bitstrings for which this equation does not hold. Verify the non-linearity of S_1 by finding a pair of bitstrings which do not satisfy the above equality. (**Hint**: This problem is really easy.)

5. This problem is based on Stinson's problem 2.29, p.58. Please follow Stinson's instructions for the problem, but instead of using his ciphertext, use this one:

```
TOSIEBCBBPKZINTEKMKEZTIBIMTSXM
FADGZETGXIQWUQSVFTVCPWRSQHGXLL
BVGFBDIWKDTBJXDFLBKVLSWEMMGONF
AKIHTZXRNLPHCCTJAVWNSKMMUTEHCD
BVJLPJWPFPXTGHWSGBBSORPJLSFEID
WNXTUZKLEHLPYEFHXNGUUMBNCRHIXV
MZVLCGDAXMOWDCCICSUFQMGJOSIARG
YIVOHLQIMJPWOACFDJHDXIVPGWVXLT
AZAPYTMIHRTYRDBXOWCFVSLHCZEYNT
UNEVBIBSETLJWPFQQEEOECFFOEUEVZ
WWKSWPXAOGXFGNAVZABEFHZTICODZH
EWKFQO
```

6. Let

$M = 1110100101110101001110101101010101110111010111010111110010010100$

be a DES plaintext message, and let

$C = 1011111111100000101001000111111010000000010011101011110110110001$

be the DES output after two rounds. Assume that the initial permutation IP was not applied. Thus, according to our usual notation, M is the concatenation of L_0 and R_0, while C is the concatenation of L_2 and R_2. (That is, C consists of L_2 *followed by* R_2; and similarly for M.)

i. Explain how to use this information to find the set of 6-bit strings that are the possible values of the first six bits of K_1, the round key for the first round. (There's nothing special about the first six bits; you can apply similar reasoning to any of the six-bit substrings of K_1. And you can apply this reasoning to K_2 as well as to K_1. But for this problem, I'm just asking you to focus on the first substring of K_1.)

ii. Apply the method you describe in (i) to actually find the set of 6-bit strings that are the possible values of the first six bits of K_1. (There will be more than one possible value.)