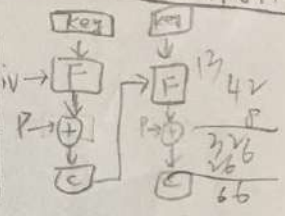
Introduction to Cryptography, 2021 Spring

Midterm, 4/16/2021 (Friday)

1. (10%) Solve the equation 184x+57y=1 for integers x and y by filling in the following table with the extended Euclidean algorithm, where $184x_i + 57y_i = r_i$ for all $i \geq -1$

i	r_i	q_i	x_i	y_i
-1	184		1	0
0	57		0	1
1	...	...	...	...
...	...	...	...	...



2. (10%) Solve x, $0 \leq x < 546$, for the system: x mod 6=2, x mod 7=4 and x mod 13 = 1 by the Chinese Remainder Theorem.

3. (10%) Compute the gcd of polynomials $6x^4+6x^3+4x^2+3x+2$ and $5x^5+6x^4+4x^3+x+1$ with coefficients over the finite field Z_7.

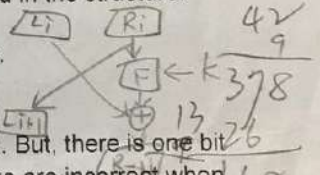
4. (10%) In AES, the byte operations are defined on the finite field $GF(2^8)/x^8+x^4+x^3+x+1$. Use the shift-and-XOR algorithm to compute 37xA6 by filling in the following table.

i	b_i	f (shift-XOR)	f (mod g(x))
Initial		0000 0000	0000 0000
7	1	...	...
...	...	...	...

Add key
Substitution
Shift
Mix

5. (15%) AES is a substitution and permutation network. Describe the 4 functions and their inverses in a round and indicate which steps are substitution and which steps are permutations.

6. (10) DES's decryption depends on the Feistel structure. Describe the Feistel structure and show that the decryption is always correct no matter what function F is used in the structure.



7. This problem is about the CFB mode for AES with the block size of s bytes.
   (a) (8%) Describe the encryption and decryption diagrams.
   (b) (5%) Assume that s=3 and $c_1\ c_2 \ldots\ c_{100}$ blocks of ciphertext are created. But, there is one bit error in each of c_2, c_5 and c_{83} during transmission. What plaintext blocks are incorrect when decryption? Show your inference.

8. This problem is about RSA.
   (a) (4%) Let n=143=11x13 and e=7. Compute the private exponent d.
   (b) (9%) Following from (a), show the speedup computation of M for the ciphertext C=8.
   (c) (9%) For any RSA parameter (n=pq, e, d), show that the ciphertext $C=M^e \bmod n$ can be decrypted correctly no matter whether M is relatively prime to n or not.