TIK-110.503 Foundations of Cryptology
Final exam
January 29, 2000

1. Who is the inventor, who borrowed the name of his new invention from the famous survivor

   `RLD ABLAIORXBLJ` ?

   At least you should be able to derive the inventor's initials, which are used as a key when the survivor's name was encrypted using the **affine cipher** on an alphabet of 27 letters. The first two letters of the survivor's name are `RO`. The plaintext and ciphertext alphabet consists of the 26 letters `A - Z` and the space between words. These 27 symbols are converted to integers modulo 27 as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	"space"
13	14	15	16	17	18	19	20	21	22	23	24	25	26

2. Plaintext is formed by independent bits arranged in blocks of eight bits. The probability that a plaintext bit equals 0 is p. Each block $x_1, x_2, \ldots, x_8$ is encrypted using one key bit z by adding it modulo 2 to each plaintext bit. Hence the ciphertext block is $y_1, y_2, \ldots, y_8$ where $y_i = x_i \oplus z$, $i = 1, 2, \ldots, 8$. It is assumed that each key bit is generated uniformly at random and independently of the plaintext. Assume you see a ciphertext block with k zeroes and $8-k$ ones, $k = 0, 1, 2, \ldots, 8$. Determine the probability that the key bit was $z = 0$. What kind of ciphertext maximizes this probability?

3. a) Give the Solovay-Strassen primality test for an odd integer n, $n > 1$.

   b) Is 21 Euler pseudo-prime to the base 2?

4. Number 29 is square root of 841. Find some other number which is square root of 841 modulo 2000. Hint: Recall that if m_1 divides $a - b$ and m_2 divides $a + b$, and $\gcd(m_1, m_2) = 1$, then $a^2 \equiv b^2 \pmod{m_1 m_2}$.

5. Consider **ElGamal Public-key Cryptosystem** in Galois field GF(2^4) with polynomial $x^4 + x + 1$ and with the primitive element $\alpha = 0010 = x$. Your private key is $a = 7$.

   a) Compute your public key β.

   b) Decrypt ciphertext (0100,1110) using your secret key. Recall that given a plaintext X the ciphertext is $(\alpha^k, X\beta^k)$ where the integer k is known only to the encryptor.