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

1. (6 points) The DES keys are 64 bits long, where each eighth bit is a parity bit computed as a modulo 2 sum of the preceding seven bits. A key management center uses DES encryption algorithm and a "master" DES key to encrypt DES keys to end users. Each ciphertext block consists of one encrypted DES key. Estimate the unicity distance of this cryptosystem, that is, estimate the average number of encrypted end users' DES keys needed to uniquely compute the master key given enough computing time.

2. (6 points) "Piling-up lemma": Let $X_1, X_2, \ldots, X_n$ be independent binary random variables and let $X = X_1 \oplus X_2 \oplus \ldots \oplus X_n$. Prove that then

$$2p - 1 = \prod_{i=1}^{n} (2p_i - 1),$$

where p_i is probability that $X_i = 0$, for $i = 1, 2, \ldots, n$, and p is the probability that $X = 0$.

3. (6 points) The integer $n = 89855713$ is known to be a product of two primes. Further, it is given that $\phi(n) = 89836740$. Find the factors of n.

4. Let p be an odd prime and let d, $d > 1$, be a divisor of $p - 1$. Consider the congruence equation

$$x^d \equiv a \,(\mathrm{mod} p),$$

where a and x are integers.

   a) (3 points) Given a, show that a solution x exists if and only if

$$a^{\frac{p-1}{d}} \equiv 1 \,(\mathrm{mod} p).$$

   b) (3 points) Show that the congruence

$$x^4 \equiv 2000 \,(\mathrm{mod} 29)$$

   does not have a solution.

5. (6 points) Consider a variation of the ElGamal signature scheme giving message recovery. The public parameters of this scheme are odd primes p and q such that q divides $p - 1$, and an element α of the field $\mathbb{Z}_p$ such that the multiplicative order of α is equal to q. A user's private key is an integer a such that $1 < a < q$, and the user's public key β is computed as $\beta = \alpha^a \bmod p$. A signature of a message $x \in \mathbb{Z}_q$ is a pair (γ, δ), where $\gamma \in \mathbb{Z}_q$ and $\delta \in \mathbb{Z}_q$ are produced as follows: The user generates a secret random integer k such that $1 < k < q$ and computes

$$\begin{aligned} \gamma &= x - (\alpha^k \bmod p) \bmod q \\ \delta &= k - a\gamma \bmod q. \end{aligned}$$

Show how the message x can be recovered from the signature (γ, δ) given the public parameters p, q, α and β.