which was enciphered using the ElGamal cryptosystem in the prime field of 2972627050091390067716119 27 elements, using your public key g^a. Your secret key is $a = 10384756843984756438549809$. Decipher the message.

9. Here is a scheme (also due to ElGamal) for sending a signature using a large prime finite field $\mathbf{F}_p$. Explain why Alice can do all the steps required to send her signature (in time polynomial in $\log p$), why Bob can verify that Alice must have sent the signature, and why the system would fail if an imposter could solve the discrete logarithm problem in $\mathbf{F}_p^*$.
We suppose that a fixed p and a fixed $g \in \mathbf{F}_p^*$ are publicly known. Each user A also chooses a random integer a_A, $0 < a_A < p-1$, which is kept secret, and publishes $y_A = g^{a_A}$.
To send her signature — which is composed of message units with numerical equivalents S in the range $0 \leq S < p-1$ — Alice first chooses a random integer k prime to $p-1$. She computes $r = g^k \bmod p$, and then solves the following congruence for the unknown x: $g^S \equiv y^r r^x \bmod p$. She sends Bob the pair (r, x) along with her signature S. Bob verifies that g^S is in fact $\equiv y^r r^x \bmod p$, and he is happy, secure in his confidence that Alice did send the message S.
10. Using the Silver–Pohlig–Hellman algorithm, find the discrete log of 153 to the base 2 in $\mathbf{F}_{181}^*$. (2 is a generator of $\mathbf{F}_{181}^*$.)
11. (a) What is the percent likelihood that a random polynomial over $\mathbf{F}_2$ of degree exactly 10 factors into a product of polynomials of degree ≤ 2? What is the likelihood that a random nonzero polynomial of degree at most 10 factors into such a product?
(b) What is the probability that a random monic polynomial over $\mathbf{F}_3$ of degree exactly 10 factors into a product of polynomials of degree ≤ 2? What is the probability that a random monic polynomial of degree at most 10 factors into such a product?
12. For $n > m \geq 1$, let $P_p(n,m)$ denote the probability that a random monic polynomial over $\mathbf{F}_p$ of degree at most n is a product of irreducible factors all of degree $\leq m$.
(a) Prove that for any fixed n and m, $P(n,m) = \lim_{p\to\infty} P_p(n,m)$ exists and is strictly between 0 and 1.
(b) Find an explicit expression for $P(n,2)$.
(c) Compute $P(n,2)$ exactly for all $n \leq 7$.

References for § IV.3

1. L. M. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," *Proc. 20th Annual Symposium on the Foundations of Computer Science* (1979), 55–60.