CSEP 590E: Practical Aspects of Modern Cryptography

Homework #6 Due: 6:30pm Nov 12, 2016

1. An early version of a zero-knowledge interactive proof follows a paradigm known as *cut and choose* — an example works as follows. I take a deck of cards and from that deck deal 10 cards face down which I assert are all spades. I then allow you to select (but not touch) any one of the 10 cards. Once you've made your selection, I turn over the other 9 cards and show you that these 9 are all spades. After the reveal, you should have at least 90% confidence that the card you selected is also a spade – even though you don't know its value.

   Let's now extend this game a bit further. Suppose that I want to be able to choose either a spade or a club without your knowing which of the two I have selected. I don't care about the value of the card, but I want to be the one to choose the suit. I also need to be able to convince you that the card that I've selected is a black suit and not one of those evil hearts or diamonds.

   Describe how I can convince you (with at least 90% confidence) that my card is black while retaining the ability to choose the suit I prefer. You should not learn the suit of my card.

   Hint: Consider interactively proving something about pairs of cards.

2. We'd now like to interactively prove something similar to the above, but with much higher confidence. Suppose that I have a large number of visually-indistinguishable objects each of which, I assert, weighs either 101 grams or 102 grams. I again want to select an object and convince you that its weight is one of the two stated values (and not some unapproved weight like 99 grams or 103 grams) – once again, without your knowing the weight of the object I've selected. However, 90% or even 99% confidence is no longer good enough. Your confidence should be at least 99.9999% (and I don't have anywhere near a million objects to play cut and choose with).

At our disposal we have two kinds of scales: an accurate scale which will tell us the precise weight of an object and a balance scale which will tell us whether or not two objects are the same weight.
Describe how I can convince you with at least 99.9999% confidence that my selected weight is either 101 or 102 grams without revealing which of the two its actual weight. How many objects do I need to make this work?

3. Suppose that a secret from the set $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ has been shared amongst 5 people using Shamir's threshold scheme by generating a polynomial $P(x) = ax^2 + bx + c$ with $c = P(0)$ as the secret value. The value given to shareholders 1 through 5 are $P(1)$, $P(2)$, $P(3)$, $P(4)$, and $P(5)$, respectively. (All operations here are "mod 11".)
At some later point, the first, third, and fourth shareholders decide to reconstruct the secret and reveal their shares to be $P(1) = 7$, $P(3) = 2$, and $P(4) = 6$.
What is the value of the secret $P(0)$?
What were the shares held by shareholders 2 and 5?
[Note: You may use a calculator and the extended Euclidean algorithm for your "mod 11" computations, but it shouldn't be necessary since multiples of 11 are easy to remember and since 12 has many factors – making most divisions easy (e.g. $\frac{1}{2} \equiv_{11} \frac{12}{2} \equiv_{11} 6$, $\frac{1}{3} \equiv_{11} \frac{12}{3} \equiv_{11} 4$, and $\frac{1}{4} \equiv_{11} \frac{12}{4} \equiv_{11} 3$).]

4. ElGamal encryption implicitly negotiates a Diffie-Hellman key exchange and immediately uses the freshly exchanged key to mask a message with multiplication. Specifically, given pre-agreed upon public parameters p and g, if Alice's private key is a, her public key is $A = g^a \bmod p$. Bob encrypts message M for Alice by randomly selecting a value e and sending Alice the pair $(r, s) = (A^e M, g^e)$. Alice then decrypts by computing
$$\frac{r}{s^a} = \frac{A^e M}{g^{ae}} = \frac{g^{ae} M}{g^{ae}} = M.$$
(All computations here, including the divisions, are "mod p".)
Suppose that in a toy example, $p = 11$, $g = 2$, and Alice's private key is $a = 8$. What is Alice's public key?
Suppose that Alice receives the encrypted message $(6,5)$ from Bob. What is the decryption of Bob's message?

Using the fact that 11 is a *really* small number and your superpower ability of *exhaustive search* on values in $\mathbb{Z}_{11}$, determine the private key that corresponds to a public key of $A = 9$.

5. Using the set up of the previous problem, suppose that Carol is watching. She wants to duplicate Bob's message to Alice (without knowing its decryption) but wants the encryption to look different so that Alice will not know that it is just a copy. To do so, she encrypts the message $M = 1$ and multiplies her encryption by Bob's encryption (componentwise). If Carol randomly selects the value $e = 3$ for her encryption, what is her encryption of the message $M = 1$? What is the resulting "re-encryption" of Bob's message (6,5)? Without decrypting the two encryptions (2,5) and (8,3) show that their decryptions are equal by taking the (componentwise) quotient of the two encryptions and showing that it decrypts to 1. Briefly describe how to use this ability to show that two encryptions will decrypt to the same value to interactively prove that a particular value is either an encryption of 1 or an encryption of 2 without revealing which is the case.