

12 Additional Material

12.1 Coin Flipping

1. **Introduction:** The whole idea of "coin flipping" is for two parties to agree that a "coinflip" is fair when they are not in the presence of the coin.
2. **Theorem:** Suppose p, q are distinct odd primes. Let $A \not\equiv 0 \pmod{n = pq}$. If $x^2 \equiv A \pmod{n}$ has any solutions (if at all) then it has 4 distinct solutions mod n .

Proof. First note that if $x^2 \equiv A \pmod{n}$ then $x^2 \equiv A \pmod{p}$ and $x^2 \equiv A \pmod{q}$. Then we know that $x^2 \equiv A \pmod{p, q}$ have exactly two solutions each. Next observe that by the CRT, solutions to $x^2 \equiv A \pmod{n}$ correspond exactly to pairs of solutions to $x^2 \equiv A \pmod{p, q}$. Why are they distinct?

- Suppose $x \equiv a \pmod{n}$ is one solution. So $a^2 \equiv A \pmod{n}$. Then, consider the system

$$\begin{aligned}x &\equiv a \pmod{p} \\x &\equiv a \pmod{q}\end{aligned}$$

by the CRT this has a unique solution mod $pq = n$. This solution will satisfy $x^2 \equiv a^2 \equiv A \pmod{p}$ and $x^2 \equiv a^2 \equiv A \pmod{q}$. Since $\gcd(p, q) = 1$ we have that $x^2 \equiv A \pmod{pq = n}$. Call this solution X .

Note that $x = -X$ is a solution as well since $(-X)^2 \equiv X^2 \equiv A \pmod{n}$. Moreover, note that $x = -x$ satisfies the system

$$\begin{aligned}x &\equiv -a \pmod{p} \\x &\equiv -a \pmod{q}\end{aligned}$$

- Now, consider this system,

$$\begin{aligned}x &\equiv a \pmod{p} \\x &\equiv -a \pmod{q}\end{aligned}$$

by the CRT this has a unique solution mod $pq = n$. Call this solution Y .

likewise, $x = -Y$ is a solution as well. Since it satisfies

$$\begin{aligned}x &\equiv -a \pmod{p} \\x &\equiv a \pmod{q}\end{aligned}$$

So, all together we have $x = X, -X, Y, -Y$ as our solution where they are all distinct mod $n = pq$. \square

3. **Theorem:** If $p \equiv 3 \pmod{4}$ and if $x^2 \equiv A \pmod{p}$ has solutions, we can find them easily.

Proof. We know if it has any, it has two. Since A is a QR we know that $\left(\frac{A}{p}\right) = 1$ and then,

$$\left(\pm A^{\frac{p+1}{4}}\right)^2 \equiv A^{\frac{p+1}{2}} \equiv A \cdot A^{\frac{p-1}{2}} \equiv A \left(\frac{A}{p}\right) \equiv A \cdot 1 \equiv A \pmod{p}$$

So we know that $x = \pm A^{\frac{p+1}{4}}$ to be the two solutions. \square

4. **Theorem:** Consider $x^2 \equiv A \pmod{n}$, if $n = pq$ and we know p, q and if there are solutions, there are 4 and we can find them easily.

Proof. Since $x^2 \equiv A \pmod{n}$ has solutions so do $x^2 \equiv A \pmod{p}$ and $x^2 \equiv A \pmod{q}$. We can find these as we have seen. They are $x \equiv \pm A^{\frac{p+1}{4}} \pmod{p}$ and $x \equiv \pm A^{\frac{q+1}{4}} \pmod{q}$. This leads us to the 4 systems in the CRT.

- We solve,

$$\begin{aligned} x &\equiv A^{\frac{p+1}{4}} \pmod{p} \\ x &\equiv A^{\frac{q+1}{4}} \pmod{q} \end{aligned}$$

Call that result X , this also gives us $-X$.

- We solve,

$$\begin{aligned} x &\equiv A^{\frac{p+1}{4}} \pmod{p} \\ x &\equiv -A^{\frac{q+1}{4}} \pmod{q} \end{aligned}$$

Call that result Y , this also gives us $-Y$.

So we have 4 solutions. \square

Ex. Suppose $p = 31, q = 43$ so $n = pq = 1333$. Suppose we know $x^2 \equiv 669 \pmod{1333}$ has solutions. Find them!

- Solve,

$$\begin{aligned} x &\equiv 669^{(31+1)/4} \equiv 7 \pmod{31} \\ x &\equiv 669^{(43+1)/4} \equiv 14 \pmod{43} \end{aligned}$$

Which gives us $X = 100 \pmod{1333}$ and $-X = 100 \pmod{1333}$.

- Solve

$$x \equiv 669^{(31+1)/4} \equiv 7 \pmod{31}$$

$$x \equiv -669^{(43+1)/4} \equiv -14 \pmod{43}$$

Which gives us $Y = 1061 \pmod{1333}$ and $-X = -1061 \equiv 272 \pmod{1333}$.

So our 4 solutions are; 100, -100, 1061, 272.

5. **Theorem:** Knowing one of $\pm X$ and one of $\pm Y$ is equivalent to factoring n .

Proof.

→ Suppose we know X and Y . Observe that $X + Y \equiv a + a \equiv 2a \pmod{p}$ (we know that $2a \not\equiv 0 \pmod{p}$ since $p \nmid 2$ and $p \nmid a$) and $X + Y \equiv a + (-a) \equiv 0 \pmod{q}$. So $q \mid (X + Y)$ and $p \nmid (X + Y)$, since if $p \mid (X + Y)$ then $p \mid 2a$ but then $p \mid a$ so $a \equiv 0 \pmod{p}$. Which leads to a contradiction. So $\gcd(X + Y, n) = q$, thus we can find q and then p follows as $p = \frac{n}{q}$. Similar arguments work for knowing X and $-Y$, $-X$ and Y , $-X$ and $-Y$.

← This is obvious, we did it above. □

6. **Process:**

- Alice picks primes p, q both congruent to 3 mod 4, both of which are distinct and odd. She finds $n = pq$. She sends n to Bob.
- Bob picks $0 < b < n$ and calculates $S \equiv b^2 \pmod{n}$. He knows that $X^2 \equiv S$ has 4 solutions but he can't find all of them since he can't factor n . He only has two solutions, which are b and $-b$. Bob then sends S back to Alice.
- Alice finds the 4 solutions to $x^2 \equiv S \pmod{n}$. She gets $X, -X, Y, -Y$, one of these corresponds to Bob's b but she does not know which.
- Alice chooses one and sends it back to Bob.
- If she sends back $\pm b$, it does not help Bob. However, if she sends back either of the others, he can factor n . If Bob can factor n he wins! (50% chance that he gets an integer that helps him factor n .)

7. **Ex.** Alice chooses $p = 31$ and $q = 43$ so $n = 1333$. She sends 1333 to Bob. Bob chooses $b = 100$, and finds $S \equiv b^2 \equiv 669 \pmod{1333}$. He then sends it to Alice, Alice solves $x^2 \equiv 669 \pmod{1333}$. She gets 100, 272, 1061, 1233 as the solutions. Alice knows that Bob's b corresponds to one of these, but she has no way of determining which one that is. She then picks one and sends it to Bob. If she sends back 100, 1233 ($\equiv -100$) Bob can't factor n . If she sends back 272, 1061 Bob can factor n , since $\gcd(100 \pm 272, 1333)$ and $\gcd(100 \pm 1061, 1333)$ will give him either 31 or 43.

12.2 El-Gamal Cryptosystem

1. **Introduction:** This system is based on the difficulty of calculating discrete logarithms. Like RSA this is asymmetric.
2. **Key Creation:** Bob chooses one large prime p , a primitive root $r \bmod p$, and an integer a with $1 \leq a \leq p-2$. He keeps a secret. He then calculates $b \equiv r^a \bmod p$. Then he makes (p, r, b) public. Observe that $a \equiv \text{ind}_r b \bmod p-1$ (this is extremely difficult to calculate).
3. **Encryption:** Suppose Alice wishes to send the plaintext block P to Bob. She first chooses a random integer k with $1 \leq k \leq p-2$, then she encrypts via $\epsilon(P) \equiv (r^k, Pb^k) \bmod p$. This produces a pair (γ, δ) which is the ciphertext, i.e. $\gamma \equiv r^k \bmod p$ and $\delta \equiv Pb^k \bmod p$.

Note: By choosing a different (randomly) k each time, we can ensure that the same P , if encrypted multiple times, will yield different ciphertext. Which can alleviate issues of frequency analysis.

4. **Decryption:** Bob receives (γ, δ) , we claim that $P \equiv \gamma^{p-1-a} \delta \bmod p$ (note that $p-1-a \geq 1$). To see this note:

$$\begin{aligned} \gamma^{p-1-a} \delta &\equiv (r^k)^{p-1-a} (Pb^k) \bmod p \\ &\equiv (r^{p-1})^k (r^a)^{-k} b^k P \bmod p \\ &\equiv (1^k) (b^{-k}) b^k P \bmod p \end{aligned}$$

mult. inverse of $r^a \exists$ since p is prime and... Some notes about the derivation above, we know $(r^a)^{-k}$ since it is the multiplicative inverse of r^a which we know exists since p is prime, furthermore we know that $r^a \equiv b$ and $b \leq p-1$ and p is prime. For $(r^{p-1})^k$ we have that $r^{p-1} \equiv 1$ since r is a primitive root. Thus we have $\epsilon^{-1}(\gamma, \delta) \equiv \gamma^{p-1-a} \delta \bmod p$.

5. **Ex.** Bob selects $p = 2539$ and $r = 2$ (a PR) and $a = 42$ (kept private). Bob calculates $b = 2^{42} \equiv 1305 \bmod 2539$, so his public key is $(p, r, b) = (2539, 2, 1305)$. Eve knows $2^a \equiv 1305 \bmod 2539$ but she can't find a (this is the problem that is hard to solve). Alice wants to send OHNO, she breaks it into 2 blocks of size 2; OH=1407, NO=1314. Then she encrypts:

1407: She chooses $k = 100$ then she does

$$\begin{aligned} \epsilon(1407) &= (2^{100}, 1407 \cdot 1305^{100}) \bmod 2539 \\ &= (613, 635) \bmod 2539 \end{aligned}$$

1314: She chooses $k = 200$ then she does

$$\begin{aligned} \epsilon(1314) &= (2^{200}, 1314 \cdot 1305^{200}) \bmod 2539 \\ &= (2356, 1494) \bmod 2539 \end{aligned}$$

So she then sends (613, 635) and (2356, 1494).

Bob then gets those and he decrypts:

$$(613, 635): \epsilon^{-1}(613, 635) \equiv 613^{2539-1-42} \cdot 635 \equiv 1407 \pmod{2539}.$$

$$(2356, 1494): \epsilon^{-1}(2356, 1394) \equiv 2356^{2359-1-42} \cdot 1494 \equiv 1314 \pmod{2539}.$$

Then he is done.

6. Comments:

- (a) To decrypt we need a , and getting this from b is hard.
- (b) In theory we could try a^x for lots of x but,
- (c) Use different k each time so if $P_1 = P_2$ we get $c_1 \neq c_2$.
- (d) Ciphertext is two times longer than the plaintext, which is a disadvantage, but it has security given above.
- (e) Typically ElGamal and RSA (asymmetric encryption schemes) are actually not used for the entire message. They are used to exchange a symmetric key which is then used to transmit data since it is fast.
- (f) Signing messages is possible but not as easy. Alice can not simply use her own d since there is no obvious mechanism for getting a random k involved.
- (g) While verifying primitive roots can be hard, Bob's PR need not be public. Alice could give it to him, in fact so could Eve!
- (h) Alice should definitely use a different (random) k each time. If Alice uses the same k for P_1 and P_2 then *if* Eve figures out P_1 she can figure out P_2 . This is because Eve will know $\gamma_1 \equiv P_1 b^k$ and $\gamma_2 \equiv P_2 b^k$ then observe that $P_2 \equiv \gamma_2 (b^k)^{-1} \equiv \gamma_2 (\gamma_1 P_1^{-1})^{-1} \equiv \gamma_2 \gamma_1^{-1} P_1 \pmod{p}$.

12.3 Problems

1. Use Pollard's Rho method to obtain a factor of each of the following. Use $x_0 = 2$ and $x_{n+1} = x_n^2 + 1$.
 - (a) $n = 143$
 - (b) $n = 5473$
 - (c) $n = 234643$
2. From the context of class and notes, show that knowing X and $-Y$ is enough to factor n .

3. Emulate/rewrite the final coin-flip example from class with $p = 67$, $q = 83$, and $b = 123$. Describe Alice's choices, Bob's choice, who sends what to whom, the equation Alice solves, what those solutions are, and what possibilities might emerge.

For the equation Alice solves write down the details as in the example of Theorem 3 in the notes but you can use technology to do the gritty calculations.

4. These relate to the El-Gamal Cryptosystem

- (a) Choose a prime p with $2525 < p < 10000$ (just hunt for lists of primes on the internet) and find a primitive root r of p . Don't do this just by googling, do this by making sure you understand what a primitive root is (what properties must it have?) and by sampling some possibilities (Wolfram Alpha can help) until you find one. Make sure you explain the process you followed so it's clear to the grader how you tested and validated. If you're not sure how to do this, ask!
- (b) Choose some a with $0 \leq a \leq p - 1$ and find the least nonnegative residue $b \equiv r^a \pmod{p}$. What is your public key?
- (c) Create a message of your choosing with between 15 and 20 characters and encrypt it. Show as much work as we do in class, the actual calculations can be done elsewhere.