The University of Sydney
Math3925 Public Key Cryptography

Semester 2 **Solutions for Assignment 1** 2004

This assignment will be due on Friday 3 September, should be submitted at 638 Carslaw by 5PM, and is worth 10% of the assessment for this course.

1. Let n be the integer 308060837760896562 7, and define $\pi : \mathbb{Z}^8 \to \mathbb{Z}/n\mathbb{Z}^*$ to be the homomorphism taking the canonical basis of $\mathbb{Z}^8$ to the generators

$$\{-1, 2, 3, 5, 7, 11, 13, 17\}.$$

Verify that the rows of the matrix

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 396 & -214 & -386 & 36 & 25 & -144 & 426 \\ 1 & -205 & -34 & -196 & 230 & 83 & -662 & 19 \\ 1 & -305 & 528 & -358 & -250 & 73 & 38 & 277 \\ 1 & 38 & -45 & -282 & 584 & 122 & -24 & -476 \\ 0 & 127 & 131 & 119 & 369 & -633 & 152 & -275 \\ 0 & 436 & -54 & -138 & -442 & 330 & -312 & -350 \\ 1 & 82 & 757 & 102 & 372 & 111 & -248 & 258 \end{bmatrix}.$$

determine a map $\phi : \mathbb{Z}^8 \to \mathbb{Z}^8$ with image in the kernel of π.

a. Determine the factorization of n, and the group structure of $\ker(\pi)/\phi(\mathbb{Z}^8)$.

b. Compute the 2-torsion subgroup of $\mathbb{Z}/n\mathbb{Z}^*$.

c. Use the above relation matrix to compute an exact sequence

$$1 \to \mathbb{Z}^8 \to \mathbb{Z}^8 \to \mathbb{Z}/n\mathbb{Z}^*[2] \to 1.$$

Solution

a. Reducing the above matrix modulo 2, we find the kernel (on the left) to be spanned by vectors $\{v_1, v_2, v_3, v_4\}$

$$\begin{aligned} v_1 &= (1, 0, 0, 0, 0, 0, 0, 0) \\ v_2 &= (0, 1, 0, 0, 1, 0, 0, 1) \\ v_3 &= (0, 0, 1, 1, 0, 0, 0, 0) \\ v_4 &= (0, 0, 0, 0, 0, 0, 1, 0) \end{aligned}$$

Since for any v in this kernel, $vM = (0, 0, 0, 0, 0, 0, 0, 0, 0)$, if we lift the coordinates to the integers we can form the corresponding product vM as a linear combination of the rows of M with even coordinates. Dividing by two we obtain an element u of $\mathbb{Z}^8$ such that $\pi(2u) = \pi(u)^2 = 1$, i.e. u is a 2-torsion element. The elements u_i corresponding to the basis elements v_i are:

$$u_1 = \frac{v_1 M}{2} = (1, 0, 0, 0, 0, 0, 0, 0),$$

$$u_2 = \frac{v_2 M}{2} = (1, 258, 249, -283, 496, 129, -208, 104),$$

$$u_3 = \frac{v_3 M}{2} = (1, -255, 247, -277, -10, 78, -312, 148),$$

$$u_4 = \frac{v_4 M}{2} = (0, 218, -27, -69, -221, 165, -156, -175),$$

and their images in $\mathbb{Z}/n\mathbb{Z}^*$ are:

$$\begin{aligned}
\pi(u_1) &= 3080608377608965626,\\
\pi(u_2) &= 802583131117620736,\\
\pi(u_3) &= 1,\\
\pi(u_4) &= 802583131117620736.
\end{aligned}$$

The first element is -1, but the second and fourth give us nontrivial 2-torsion elements, from which we can factor n:

$$\begin{aligned}
\mathrm{GCD}(802583131117620736 - 1, n) &= 767205289\\
\mathrm{GCD}(802583131117620736 + 1, n) &= 4015363843
\end{aligned}$$

In order to find the group structure $\ker(\pi)/\phi(\mathbb{Z}^8)$ we will computer the full matrix of relations. In retrospect we will see that this full computation is not needed.

In the previous part we found $\pi(u_2) = \pi(u_4)$ and $\pi(u_3) = 1$, hence $u_2 - u_4$ and u_3 are new relations:

$$\begin{gathered}
(1, -255, 247, -277, -10, 78, -312, 148)\\
(1, 40, 276, -214, 717, -36, -52, 279)
\end{gathered}$$

Appending this to the known relations and reducing to a basis (say by LLL reduction) we find a new basis matrix of relations:

$$\begin{bmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 50 & -281 & 81 & 240 & 5 & -350 & -129\\
1 & -255 & 247 & -277 & -10 & 78 & -312 & 148\\
0 & 42 & 481 & 316 & -345 & 147 & -196 & -21\\
0 & 396 & -214 & -386 & 36 & 25 & -144 & 426\\
0 & 228 & -112 & -330 & -322 & -494 & -252 & 20\\
0 & 681 & 256 & -156 & 45 & 211 & 298 & -90\\
1 & -257 & -74 & -345 & -143 & 236 & -284 & -607
\end{bmatrix}.$$

Repeating the calculation of the kernel modulo 2 of this new matrix, we find the same row vectors mapping to the 2-torsion subgroup, plus a new vector which maps to 1:

$$(0, 114, -56, -165, -161, -247, -126, 10).$$

Repeating this process we find another element of the kernel of π:

$$(1, 313, -206, -378, -70, 225, 108, 108).$$

Repeating once more, we find that the kernel modulo 2 contains only those vectors which map under π to the 2-torsion.

Up to this point it has not been necessary to use the factorization of n. We know that the group order of $\mathbb{Z}/n\mathbb{Z}^*$ is $(p-1)(q-1)$ where $n = pq$. However, we find that the determinant of the basis of known kernel elements is five times larger. Thus we repeat the above procedure by finding a generator for the kernel of M modulo 5, in order to find an element $v = 5u$ in $5\mathbb{Z}^8$ which is in the kernel of π. Since five does not divide the group order, in fact this element

$$u = (1, -20, 134, -161, -364, 53, -62, -13),$$

itself must lie in $\ker(\pi)$. Adjoining this to our set of relations and row reducing yields the complete basis matrix for $\ker(\pi)$:

$$N = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 114 & -56 & -165 & -161 & -247 & -126 & 10 \\ 1 & -204 & 65 & -273 & 87 & -22 & -124 & -147 \\ 0 & 51 & -182 & 4 & 97 & -100 & 188 & -295 \\ 1 & -20 & 134 & -161 & -364 & 53 & -62 & -13 \\ 1 & -84 & -91 & 85 & 37 & 305 & -286 & -152 \\ 0 & 305 & 16 & -178 & 239 & -3 & -214 & -24 \\ 0 & 28 & -356 & -39 & 55 & 175 & 384 & 145 \end{bmatrix}$$

The group structure of $\ker(\pi)/\phi(\mathbb{Z}^8)$ can now be determined by expressing the rows of the original matrix M in terms of the rows of N which spanning $\ker(\pi)$. Explicitly, one computes MN^-1. This gives a basis matrix for $\phi(\mathbb{Z}^8)$ as a subgroup of $\ker(\pi)$. From this basis we find

$$\ker(\pi)/\phi(\mathbb{Z}^8) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}.$$

Simplification: Alternatively we can compute $\det(M) = 80|\mathbb{Z}/n\mathbb{Z}^*|$ as soon as we know the factorization of n. From the fact that the dimension of the kernel of the reduction of M modulo 2 is 4, the group structure follows. Specifically, the group $\mathbb{Z}/n\mathbb{Z}^*[2]$ has dimension 2 as a vector space, so a 2-dimensional subspace, (a group of order 4) must come from 2-torsion in the group $\ker(\pi)/\phi(\mathbb{Z}^8)$. Since we know the group has order 80, the only possible group structure with 2-torsion of order 4 is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$.

Simplification #2: If $n = pq$ where $p = 3 \bmod 4$ and $q = 3 \bmod 4$, then $\mathbb{Z}/n\mathbb{Z}^*$ has order $4r$ for some r. Then the composition $[r] \circ \pi = \pi \circ [r]$ of π with $[r]$ would give the required surjection $\mathbb{Z}^8 \to \mathbb{Z}/n\mathbb{Z}^*[2]$. The map $\mathbb{Z}^8 \to \mathbb{Z}^8$ would be any map with image $\phi(\mathbb{Z}^8) + 2\mathbb{Z}^8$. In this case, however, $p = 1 \bmod 4$ so this trick doesn't apply.

b. Let $\psi : \mathbb{Z}^8 \to \mathbb{Z}^8$ and $\rho : \mathbb{Z}^8 \to \mathbb{Z}/n\mathbb{Z}^*[2]$ be the maps giving the exact sequence desired. Since we have computed the kernel of π, we define ϕ to be given by the matrix N above, so that the following sequence is exact:

$$1 \to \mathbb{Z}^8 \xrightarrow{\phi} \mathbb{Z}^8 \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z}^* \to 1.$$

The homomorphism ρ will be the compositum of an isomorphism

$$\iota : \mathbb{Z}^8 \to \pi^{-1}(\mathbb{Z}/n\mathbb{Z}^*[2])$$

with the map π. The map ψ will have image equal to the kernel of ρ. In order to find ι we adjoin two elements

$$(1, 0, 0, 0, 0, 0, 0, 0),\ (1, 258, 249, -283, 496, 129, -208, 104).$$

generating the kernel. By basis reduction we find a set of eight vectors which determine the image of the generators for $\mathbb{Z}^8$.

Simplification: This entire calculation can again be bypassed, if we recognise that any map from $\rho : \mathbb{Z}^8 \to \mathbb{Z}/n\mathbb{Z}^*[2]$ is determined by the images of its eight generators. Since $\mathbb{Z}/n\mathbb{Z}^*[2]$ is generated by -1 and 802583131117620736, we send the first two generators of $\mathbb{Z}^8$ to -1 and 802583131117620736, respectively, and the remainder to 1. Then the inclusion with basis matrix:

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

determines a map $\psi : \mathbb{Z}^8 \to \mathbb{Z}^8$ with image equal to the kernel of ρ as required. The previous construction in terms of ϕ and π must differ from this direct construction only by a change of basis for $\mathbb{Z}^8$.

2. **a.** Prove that the integer

$$8639867736879276806755645245631174 3331$$

is composite.

b. Prove that the integer

$$360330318711888192152950419440298970 39$$

is prime, and that 3 is a primitive element.

Solution

a. For this integer n, we find that $2^{n-1} \bmod n$ equals

$$751365743068144029226833970254171276 8.$$

b. For this integer p, we find that the factorization of $p-1$ is

$$2 \cdot 3^2 \cdot 43 \cdot 4049 \cdot 33311 \cdot 3451631294607644666165892 83.$$

We check that $3^{p-1} \bmod p$ equals 1, so 3 has order dividing $p-1$. However for each $m = (p-1)/r$, where $r = 2$, 3, 43, etc. runs through the prime divisors of $p-1$, we find the $3^m \bmod p$ is not one:

$$\begin{array}{l} 36033031871188819215295041944029897038 \\ 26196303998461744328183977577030316695 \\ 28877141472703870017743095112949724239 \\ 16924899364389785081988486838678995925 \\ 12185493681708568683787524620158562757 \\ 35997470466162411157077430182287272757 \end{array}$$

Thus the order of 3 is exactly $p-1$. Consequently p is prime and 3 is primitive. Note that to complete the proof, one needs the recurse on the proof that each of the prime divisors of $p-1$ is in fact prime. Primes up to some fixed bound (e.g. $10, 100, \dots, 10^6$, etc.) can be proven by prior sieving method. We omit this recursion on the divisors of $p-1$.

3. Given the integer $n = 98424217707782056843$, find a set of generators for $\mathbb{Z}/n\mathbb{Z}^*$. Find the subgroup $H = \mathbb{Z}/n\mathbb{Z}^*[2]$ and a group G together with a homomorphism $\chi : \mathbb{Z}/n\mathbb{Z}^* \to G$ making an exact sequence

$$1 \to H \longrightarrow \mathbb{Z}/n\mathbb{Z}^* \xrightarrow{[2]} \mathbb{Z}/n\mathbb{Z}^* \xrightarrow{\chi} G \to 1.$$

Solution The factorization of n is $523 \cdot 1830013 \cdot 102836220757$. Since the 2-torsion subgroup H consists of elements which are ± 1 modulo each of these primes, and we can take as generators those with images $(-1, 1, 1)$, $(1, -1, 1)$, and $(1, 1, -1)$ in

$$\mathbb{Z}/523\mathbb{Z}^* \times \mathbb{Z}/1830013\mathbb{Z}^* \times \mathbb{Z}/102836220757\mathbb{Z}^*,$$

with respect this these three primes. Using the Chinese remainder theorem, we find their representatives in $\mathbb{Z}/n\mathbb{Z}^*$ are

$$\begin{array}{l} (-1, 1, 1) \mapsto 31616192303838213289, \\ (1, -1, 1) \mapsto 83451526506434449465, \\ (1, 1, -1) \mapsto 81780716605291450933. \end{array}$$

Thus $H = \ker([2])$ is the 2-torsion subgroup of order 8 generated by these three elements. We now define $G = \{\pm 1\}^3$ to be the multiplicative group of order 8 (which we can identify with a subgroup of $\mathbb{Z}/523\mathbb{Z}^* \times \mathbb{Z}/1830013\mathbb{Z}^* \times \mathbb{Z}/102836220757\mathbb{Z}^*$). The homomorphism from $\mathbb{Z}/n\mathbb{Z}^*$ is defined to each components is

$$\begin{aligned} x &\mapsto x^{261} \bmod 523 \\ x &\mapsto x^{915006} \bmod 1830013 \\ x &\mapsto x^{51418110378} \bmod 102836220757. \end{aligned}$$

Since the maps

$$1 \to \langle 1, -1 \rangle \xrightarrow{[2]} \mathbb{Z}/p\mathbb{Z}^* \to \mathbb{Z}/p\mathbb{Z}^* \xrightarrow{\chi_p} \langle 1, -1 \rangle \to 1$$

defined by $\chi_p(x) = x^{(p-1)/2}$ is exact, we conclude also that the the map χ is surjective and has kernel equal to the image of $[2]$, hence the sequence of homomorphisms is exact.

4. **a.** Given an RSA public key (n, e), explain how the knowledge of the RSA private key (n, d) is probabilistically polynomial time equivalent to the factorization of n by describing an algorithm to factor n.

b. Let n be the RSA modulus

$$\begin{array}{c} 25532321858816610959279818995988432629309732702730503081753 0 \\ 747345240251392473791503642932659593815276200068924379830529, \end{array}$$

with public key $(n, e) = (n, 17)$ and private key (n, d) with d equal to

$$\begin{array}{c} 240304205730038691381457119962244071805268072496287087828 26 \\ 2885567034957139042736053989307424852494087454007644144753201. \end{array}$$

Find a factorization of n.

Solution

a. By construction, $a^{ed} = a$ for every a in $\mathbb{Z}/n\mathbb{Z}$. In particular this means that $ed = 1 \bmod m$, where m is the exponent of the group $\mathbb{Z}/n\mathbb{Z}^*$ (note that m divides the order $\varphi(n)$ of $\mathbb{Z}/n\mathbb{Z}^*$ but $ed = 1 \bmod \varphi(n)$ is not strictly necessary).

In particular we may apply the following algorithm:

1. let $ed - 1 = 2^s r$ for r odd
2. choose a at random in $\mathbb{Z}/n\mathbb{Z}^*$ and set $u_1 = a^r$
3. if $u_1 = \pm 1$ then return to 2.
4. for i in $[1, \ldots, s]$ {
    set $u_2 = u_1^2$
    if $u_2 = -1$ then
        return to 2.
    if $u_2 = +1$ then
        return $\mathrm{GCD}(u_1 - 1, n)$
  }

Since $a^{ed-1} = 1$, in the course of the algorithm either $u_2 = 1$ or $u_2 = -1$ occurs. If n is not prime (as is the case in the RSA protocol), then we expect to find a 2-torsion element u_1 ($u_2 = 1$) with probability at least $1/2$.

b. We find $ed - 1 = 2^6 r$ for an odd r, but with $a = 2$ we find that $2^r \bmod n$ equals -1 which gives no information. However $u_1 = 3^r \bmod n$ is a nontrivial 2-torsion element, and $\mathrm{GCD}(u_1 - 1, n)$ picks out the factor:

$$208837501874423119625643364067739053302302858700895305581467$$

while the other factor is $\mathrm{GCD}(u_1 + 1, n)$:

$$1222592763735009121258802915225781634738005421484907170448787$$

Note that 2 and 3 play the role of "random" elements.