The University of Sydney
Math3925 Public Key Cryptography

Semester 2 **Exercises for Week 8** 2004

1. Let $n = p_1^{n_1} \cdots p_t^{n_t}$ be an odd composite number, and for each i write $p_i - 1 = 2^{k_i} r_i$ with each r_i an odd number. Justify the probabilities

$$P(x^{2^j r} = -1) = \frac{1}{m} \prod_{i=1}^{t} \frac{1}{2^{k_i - j}}$$

where $x \in \mathbb{Z}/n\mathbb{Z}^*$ (chosen uniformly at random), $j < k_i$, and where m is the largest odd divisor of $|(\mathbb{Z}/n\mathbb{Z}^*)^r|$ for any odd number r.

2. Recall the Miller–Rabin primality test:

1. let $n - 1 = 2^s r$ for r odd
2. choose a at random in $\mathbb{Z}/n\mathbb{Z}^*$ and set $u = a^r$
3. if $u = \pm 1$ then return *probable prime*
4. for i in $[1, \ldots, s-1]$ {
    set $u = u^2$
    if $u = -1$ then
        return *probable prime*
    if $u = +1$ then
        return *composite*
   }
5. return *composite*

and explain why the sum

$$P(x^r = 1) + P(x^r = -1) + P(x^{2r} = -1) + \cdots + P(x^{2^{s-1} r} = -1)$$

gives the probability that the output is *probable prime*.

3. For each of the following integers $15 = 3{\cdot}5$, $21 = 3{\cdot}7$, 29, $85 = 5{\cdot}17$, $105 = 3{\cdot}5{\cdot}7$, and $357 = 13{\cdot}29$, determine the probability that the Miller–Rabin primality test returns *probable prime*.

4. Explain what happens when $j \geq k_i$ for some i, and demonstrate this with one of the above integers.