6.857
NETWORK AND COMPUTER SECURITY
RECITATION 2

LECTURER: ADA RALUCA POPA
SCRIBE: JOHN WANG

1. Fast Exponentiation

1.1. Euler's Theorem.
Theorem: Take any element $a \in \mathbb{Z}_n^*$, then for all $n \in \mathbb{N}$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is the order of the group.

Corollary: $\forall n \in \mathbb{N}$ and $\forall a \in \mathbb{Z}_n^*$, we have $a^d \equiv a^{d \mod \phi(n)} \pmod{n}$.

For any prime p, we have $\phi(p) = p - 1$. As a consequence, we obtain *Fermat's Little Theorem:* $a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod{n}$.

1.2. Exercises with Euler's Theorem.

$$3^{25} \pmod{13} = 3^{25 \mod 12} = 3 \mod 13 \tag{1}$$

$$7^10 \mod 10 \equiv 7^{10 \mod 4} \mod 10 \equiv 9 \mod 10 \tag{2}$$

Because we know that $10 = (2)(5)$ so that $\phi(10) = \phi(2)\phi(5) = 4$.

2. Chinese Remainder Theorem

Theorem: For all $m_1, \ldots, m_r < N$ where $gcd(m_i, m_j) = 1$ for all i, j, $m = m_1 \ldots m_r < N$, and for all $a_1, \ldots, a_r < N$, there exists an integer y such that

$$y \equiv a_1 \mod m_1 \tag{3}$$
$$y \equiv a_2 \mod m_2 \tag{4}$$
$$\vdots \tag{5}$$
$$y \equiv a_r \mod m_r \tag{6}$$

Moreover, y is easy to find (can be found in $\theta(\log N)$.

2.1. Proof of CRT.

(1) $n_i = \frac{m}{m_i}$ for all i. So for instance $n_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_r$.
(2) Compute b_i which is the inverse of $n_i \mod m_i$. So compute $b_i n_i \equiv 1 \mod m_i$. We know that if $gcd(c, d) = 1$, then $cx + dy \equiv 1 \mod d$, which implies $cx \equiv 1 \mod d$. But we know that $gcd(n_i, m_i) = 1$ because all of the factors of n_i are m_j where $j \neq i$ and we have pairwise $gcd(m_i, m_j) = 1$.
(3) $y = \sum_i n_i b_i a_i \mod m$

Proof: Straightforward, see wikipedia.

2.2. Example.
Find y such that $y \equiv 6 \mod 7$ and $y \equiv 8 \mod 11$.

We can do this by using CRT. We know $a_1 = 6, a_2 = 8, m_1 = 7, m_2 = 11$. So $n_1 = 11$, $n_2 = 7$. Now we can compute the inverses, $b_1 = 2$ because $2(11) \equiv 1 \mod 7$ and $b_2 = 8$ because $8(7) \mod 11$. So we know that $y = (11)(2)(6) + (7)(8)(8) \mod 77 = 41 \mod 77$.