EXERCISES 8, TMA4160 - KRYPTOGRAFI

Ch. 5

10. Let $n = pq$ for two distinct odd primes and $ab \equiv 1 \mod \phi(n)$. RSA encryption is given by $e(x) = x^b \mod n$ and decryption by $d(y) = y^a \mod n$. This holds for any $x \in \mathbb{Z}_n^*$. Now let $x \in \mathbb{Z}_n$, we need to show that $d(e(x)) = x^{ab} = x \mod n$. From the hint, the Chinese remainder theorem ensures that it suffices to show that $x^{ab} \equiv x \mod p \wedge x^{ab} \equiv x \mod q$. By assumption $ab - 1 = k(p-1)(q-1)$ for any k, so that $x^{ab} = x \cdot x^{ab-1} = x \cdot x^{k(p-1)(q-1)} \equiv x \mod p$ from Fermat's theorem. The same argument shows that this holds modulo q as well giving the desired conclusion.

11. Set $n = pq$ for distinct odd primes and

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}$$

Now require that $ab \equiv 1 \mod \lambda(n)$ in the RSA cryptosystem.

a) We prove that $d(e(x)) = x$ with this modification; That is $x^{ab} \equiv x \mod n$. Set $d = \gcd(p-1, q-1)$. By definition $d|p-1$ and $d|q-1$. Again we use the Chinese remainder theorem in the same way as the previous exercise: $x^{\lambda(n)} = x^{(p-1)\cdot((q-1)/d)} = x^{(q-1)\cdot((p-1)/d)}$. This implies that $x^{\lambda(n)} \equiv 1 \mod p$ and $x^{\lambda(n)} \equiv 1 \mod q$ so $x^{\lambda(n)} \equiv 1 \mod n$ and since $ab \equiv 1 \mod \lambda(n)$ the conclusion follows.

b) Let $p = 37, q = 79$ and $b = 7$, then $\lambda(pq) = 468$ and $7a \equiv 1 \mod 468$ gives $a = 67$. In the original RSA we have $7a \equiv 1 \mod 2808$ so that $a = 2407$.

13. Suppose that $d_K(y) = y^d \mod n$ where $n = pq$. Define $d_p = d \mod p-1$, $d_q = d \mod q-1$, $M_p = q^{-1} \mod p$ and $M_q = p^{-1} \mod q$.

a) Set $x_p = y^{d_p} \mod p$ and similarly $x_q = y^{d_q} \mod q$. The solution to this system is found by the Chinese remainder theorem to be $x = M_p q x_p + M_q p x_q \mod n$. Note that since $d_p - d = k(p-1)$ for some k we have $y^d = y^{d_p - k(p-1)} \equiv y^{d_p} \mod p = x_p$ from Fermat's theorem. Similarly we have $y^d = y^{d_q - k(q-1)} \equiv y^{d_q} \mod q = x_q$. That is:

$$y^d \equiv y^{d_p} \equiv x_p \mod p$$
$$y^d \equiv y^{d_q} \equiv x_q \mod q$$

We have shown that x solves this system and so $x \equiv y^d \mod n$.

b) Set $p = 1511, q = 2003$ and $d = 1234577$. We compute:

$$d_p = 907$$
$$d_q = 1345$$
$$M_p = 777$$
$$M_q = 973$$

c) Given $y = 152702$ we use Algorithm 5.15 in the book to decrypt this ciphertext. Firstly $x_p \equiv 242 \mod p$ and $x_q \equiv 1087 \mod q$, we then calculate $x = 1443247 \mod n$.

15.

a) Since (b, n) is public all Oscar need to do is to compute a table for the different values of plaintext and match it up to the corresponding ciphertext.

b) Compute the table:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	6400	18718	17173	1759	18242	12359	14930	9	6279	2608	4644
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4845	1375	13444	16	13663	1437	2940	10334	365	10789	8945	11373	5116

So we see that the plaintext is "vanilla".

Problem 5, exam 2001. Let $p < 2^{1000}$ and $q = 3 \cdot 2^n - 1$ for $500 < n < 1000$ be primes. Compute $d_n = \gcd(pq, 3 \cdot 2^n - 1)$ for $500 < n < 1000$ until a value $d_n > 1$ is found. Then this must be a factor of pq. One could also check $q_n = 3 \cdot 2^n - 1$ for primality, revealing that $n = 827$ is the only n in the specified range that makes q_n prime.