T. 5.2

Alice chooses   Bob $\longrightarrow$ Alice

- Finite field k s.t. $\# k = q$
- $P, Q \in k[x]$ s.t. $\deg P(x) = m$, $\deg Q(x) = n$.
- $e \in \mathbb{Z}_{>0}$ s.t. $\gcd(e, f) = 1$, where $f = (q^m - 1)(q^n - 1)$

Alice knows f

Alice publishes

- $e \in \mathbb{Z}_{>0}$ s.t. $\gcd(e, f) = 1$, where $f = (q^m - 1)(q^n - 1)$
- $N := PQ$, i.e. $N(x) = P(x) \cdot Q(x)$

Bob chooses

- $M(x) \pmod{P(x)Q(x)}$, where $M \in k[x]$ s.t. $\gcd(M(x), N(x))$

Bob sends

- $C(x) := M(x)^e \pmod{P(x)\,Q(x)}$

a) $\boxed{\text{Explain how Alice can decrypt the cipher text}}$

$n = pq$ in RSA, with p, q large odd primes

First note that $f = (q^m - 1)(q^n - 1)$ plays the same role as $\varphi(n)$ in regular RSA.

The decryption algorithm on Alice's side is the following:

- Compute $d = e^{-1} \pmod f$. This means that $ed = 1 + \gamma f \quad \exists \gamma \in \mathbb{Z}$ (1)
- Compute $C^d \pmod{P(x)\,Q(x)} = M$.

<u>proof:</u> $C^d \bmod PQ = (M^e)^d \bmod PQ = M^{1+\gamma f} \bmod PQ = M \cdot (M^f)^\gamma \bmod PQ$

<u>Claim:</u> $M^f \bmod PQ = 1$

Let $\mathbb{F}_1 = \frac{k[x]}{\langle P(x) \rangle}$. We have that $\# \mathbb{F}_1^* = q^m - 1$ (for Theorem 3.4.2. (3)).

Moreover, we have

$$M^{q^m - 1} \equiv 1 \pmod P \qquad (2)$$

due to Lagrange's theorem over $\mathbb{F}_1^*$

Let $\mathbb{F}_2 = \frac{k[x]}{\langle Q(x) \rangle}$. We have that $\# \mathbb{F}_2^* = q^n - 1$ $\left(\begin{matrix}\text{for Theorem} \\ 3.4.2.\ (3)\end{matrix}\right)$.

Moreover, we have

$$M^{q^n - 1} \equiv 1 \pmod{Q} \qquad (3)$$

due to Lagrange's theorem over $\mathbb{F}_2^*$

From (2) and (3) we have

$$\begin{cases} M^{q^m - 1} \equiv 1 \pmod{P} \\ M^{q^n - 1} \equiv 1 \pmod{Q} \end{cases} \Longrightarrow M^{(q^m - 1)(q^n - 1)} = M^f \underset{\text{CRT}}{\equiv} 1 \pmod{PQ} \checkmark$$

Therefore, we have

$$C^d \bmod PQ = (M^e)^d \bmod PQ = M^{1 + \gamma f} \bmod PQ = M \cdot (M^f)^\gamma \bmod PQ \overset{\text{Claim}}{=} M \quad \square$$

b) $\boxed{\text{Explain briefly why this protocol is insecure}}$

Eve knows the ciphertext C, the public key $N(x) \in k[x]$ and the value of $q = \# k$.

Eve can factor $N(x) = P(x) \cdot Q(x)$ in an efficient way via Berlekamp's algorithm, that has expected polynomial runtime in $\log q$ (from the lecture notes).

the input polynomial is already SQUARE-FREE and its factors are IRREDUCIBLE

Eve can therefore recover a SQUARE-FREE IRREDUCIBLE factor of $N(x)$, that can be either $P(x)$ or $Q(x)$. Let's say that Eve recovers $P(x)$ without loss of generality.

Thus, Eve recovers $m = \deg P(x)$ and $n = \deg Q(x) = \deg N(x) - \deg P(x)$.
So, Eve has recovered $m, n \in \mathbb{Z}_{>0}$.

Therefore, Eve can compute $f := (q^m - 1)(q^n - 1)$ since q is publicly known.

With the knowledge of f, Eve can compute

$$d \equiv e^{-1} \pmod{f}$$

So Eve has recovered Alice's secret key and can decrypt using the same algorithm that Alice would (described in part a.):

$$C^d \equiv M^{ed} \underset{ed \equiv 1 \pmod{f}}{\equiv} M \pmod{P(x) \cdot Q(x)}.$$