18.6.7

9.1 (i) What is the purpose of the random part in the signature generation?

9.3 (iv) – (vi)

9.1

9.1 ElGamal

keypair: $(a = g^{\alpha})$

Sign: $\beta \in_R \mathbb{Z}_\ell : b = g^\beta$

$\gamma \in_R \mathbb{Z}_\ell^\times$

$\ell = \operatorname{ord} g$

$\alpha b^* + \beta\gamma = h(m) \text{ in } \mathbb{Z}_\ell$

$a^{b^*} \cdot b^{\gamma} = g^{h(m)} \text{ in } G$

Signing equation

Usually: $\mathbb{Z}_p^\times \ni g$

often: $\ell = \operatorname{ord} g$ is prime.

Here: $\operatorname{ord} g = p - 1$ is not prime

but: it contains a large prime.

(i) β protects the secrecy of α!

(ii) If an attacker can find β, then he can also find α and thus break the scheme.

18.6.7
12

(iii) $132622 \cdot \beta = \underbrace{\dots}_{\text{even}}$ in $\mathbb{Z}_{311302}$

$\frac{132622}{2} \cdot \beta = \frac{\dots}{2}$ in $\mathbb{Z}_{\frac{311302}{2}}$

$\beta = 140767$ in $\mathbb{Z}_{\frac{311302}{2}}$

$\beta_1 = 140767 + 0 \cdot \frac{311302}{2}$ in $\mathbb{Z}_{311302}$

$g^{\beta_1} = b$

$\beta_2 = 140707 + 1 \cdot \frac{311302}{2}$ in $\mathbb{Z}_{311302}$

$g^{\beta_2} = -b \neq b.$

(iv) The major difference that
Q needs to know the secret key α.
→ hidden channel is "only" a symmetric encryption scheme.

18.6.7

(iii) $\#K \sim p_k = \frac{1}{\#K} \rightarrow E(N_k) = \frac{1}{p_k} = \#K$. [3]

(iv)/(v)/(vi)

$$\text{average}_k \; E(N_k) = \sum_k p_k \cdot \frac{1}{p_k}$$

$$= \sum_k 1$$

(iv) Test

1. k ~~=~~ rand(0)
2. JZOO (k)

$\sum_k 1$

$\#K$.

(iv): $k=1 \quad p = \frac{1}{501} \quad : \quad E(N_1) = 501$

$k=2 \quad p = \frac{500}{501} \quad : \quad E(N_2) = \frac{501}{500} \approx 1.$