

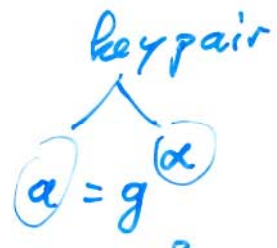
9.1 (i) What is the purpose of the random part in the signature generation?

9.3 (iv) - (vi)

9.1

9.1

ElGamal



Sign:  $\beta \in \mathbb{Z}_e$  :  $b = g^\beta$   
 $\gamma \in \mathbb{Z}_e \neq 0$

$$\alpha b^\gamma + \beta \gamma = h(m) \pmod{e}$$

$$a^{b^\gamma} \cdot b^\beta = g^{h(m)} \pmod{e}$$

Signing equation

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

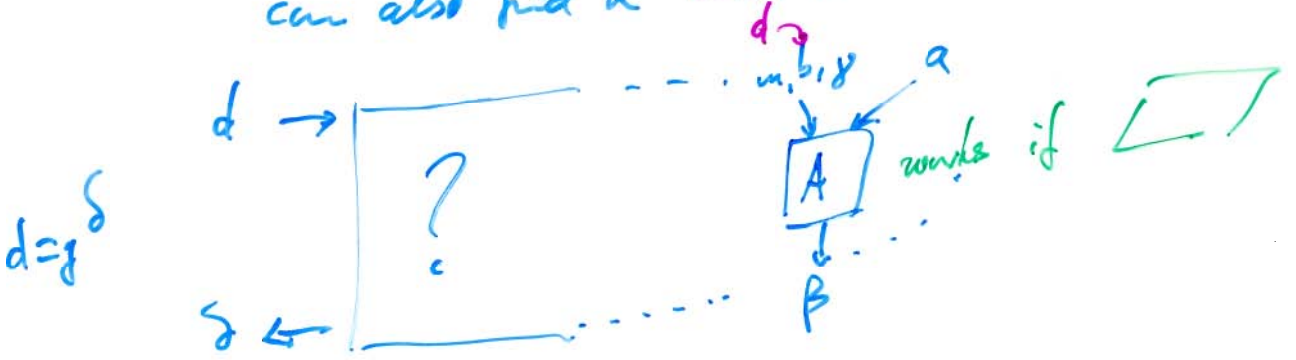
often:  $e = \text{ord } g$  is prime.

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

but: it contains a large prime.

(i)  $\beta$  protects the secrecy of  $\alpha$ !

(ii) If an attacker can find  $\beta$ , then he can also find  $\alpha$  and thus break the scheme.



(ii)

$$132622 \cdot \beta = \frac{\dots}{\text{even}} \quad \text{in } \mathbb{Z}_{311302}$$

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

$$\beta = 140707 \quad \text{in } \mathbb{Z}_{\frac{311302}{2}}$$

$$\beta_1 = 140707 \in \mathbb{Z}_{311302} + 0 \cdot \frac{311302}{2}$$

$$g^{\beta_1} = b$$

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

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

(N) The major difference that Q needs to know the secret key  $\alpha$ .  
 → hidden channel is 'only' a symmetric encryption scheme.

$$(iii) \quad \#X \sim P_k = \frac{1}{\#X} \rightarrow E(N_k) = \frac{1}{P_k} = \#X. \quad \boxed{3}$$

(iv)/(v)/(vi)

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

(\*) Test

1.	$k \neq 1$ (and 0)	$\sum_k 1$
2.	JZO (k)	$\#X.$

$$(iv) : k=1 \quad P = \frac{1}{501} \quad : \quad E(N_k) = 501$$

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