Solution

Cryptography – Questionnaire 6

Name: _____

Matr.: _____

Questions

	true	false
OWF exist if and only if CCA-secure ES exist.	☒	☐
RSA "works" for $N = 35$ and $e = 3$, i.e. $x \mapsto x^e \bmod N$ is a permutation (in particular: invertible).	☐	☒
The ElGamal-PKES is CCA-secure.	☐	☒
If DDH is hard w.r.t. $\mathsf{Gen}\mathbb{G}_{\mathsf{cyc}}$ then ElGamal based on $\mathsf{Gen}\mathbb{G}_{\mathsf{cyc}}$ is CPA-secure.	☒	☐

"(One|two)-liners"

Exercise 6.1 **2P**

Briefly state why the DDH over $\mathbb{Z}_p^*$ (p prime) is *not* hard.
Answer:

- By computing the Legendre-symbol we can distinguish between an element from $\mathbb{QR}$ and one from $\mathbb{Z}_p^* \setminus \mathbb{QR}$. If g is a generator of $\mathbb{Z}_p^*$ then g^r is in $\mathcal{G}_{\mathbb{SP}}$ with prob. 1/2 (for a random r) and g^{ab} is in $\mathbb{QR}$ with prob. 3/4 (for random a, b).

Exercise 6.2 **2P**

Suppose Bob's public ElGamal key is $(\mathbb{G}, q, g, h_b) = (\mathbb{Z}_{17}^*, 16, 6, 5)$. Alice wants to send him the message $m = 7$ encrypted using the ElGamal PKES. Compute the ciphertext $c = (c_1, c_2)$ that is sent to Bob assuming Alice has generated $a = 3$ as her secret.
Answer: $c = (12, 8)$

Exercise 6.3 **2P**

Briefly state

- why RSA-based PKES use a probabilistic padding scheme and
- name one of these schemes used in practice.

Answer: Possible reasons:

- Without *randomized* padding the scheme is deterministic (and stateless, hence not CPA-secure)
- Padding is needed to prevent attacks on small messages (where no modulo-wraparound takes place)
- Randomized padding is needed to ensure that the effective message space used, is as large as the theoretical message space (compare: RSA full domain hash for signatures!).

Thus one uses for example OAEP-RSA (optimal asymmetric encryption padding).