Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Informatik
FH Zentralschweiz

I.BA_MOVK_MM – Kryptographie

Übung: Homomorphe Verschlüsselung

Dr. Ladan Pooyan-Weihs

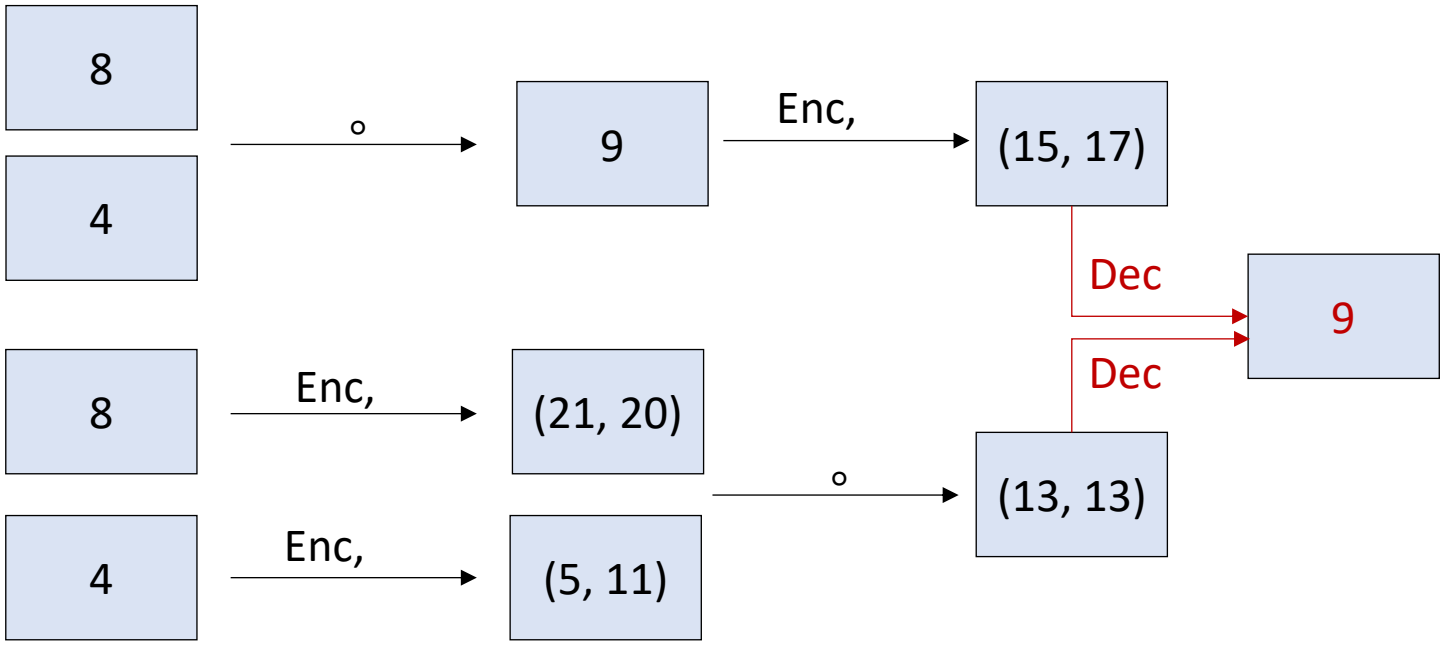
Semesterwoche 10

Aufgabe 1: Homomorphe Verschlüsselung

1. Welches der drei Verschlüsselungsverfahren (RSA, EL-GAMAL, Paillier) ist eher geeignet für die Verwendung in homomorpher Verschlüsselung eingesetzt werden? Begründen bitte Ihre Antwort?
2. Geben Sie ein Beispiel, in welchem Bereich das Paillier-Verfahren eingesetzt werden könnte? Begründen Sie Ihre Antwort?

Aufgabe 2: Homomorphie-Eigenschaft von EL-GAMAL

Berechnen Sie bitte jeden Schritt im unteren Teil des Beispiels (s. unten). Die Berechnung für den oberen Teil finden Sie auf den Folien SW10.



Aufgabe 3: Paillier-Verfahren

Gegeben sind zwei Primzahlen p=3 und q=5. Sei g = 16 aus $\mathbb{Z}^*_{225}$ zufällig gewählt.

1. Berechnen Sie jeweils den öffentlichen und privaten Schlüssel.
2. Verschlüssen Sie den Klartext m=13.
3. Entschlüssen Sie den Ciphertext c=71.

Hinweis: Das Ergebnis durch Codierung wird akzeptiert.

Viel Vergnügen!