1. MAB-RSA

1.1. Fragen: Die Formeln lauten

zum Verschlüsseln: _____ zum Entschlüsseln: _____

zum Signieren: _____ zum Verifizieren: _____

1.2. Aufgabe 1: d berechnen

Gegeben: e= 17 und phi(n)=60
Allgemein: Es gilt: e*d ≡ 1 mod phi(n)
Im Speziellen: 17*d ≡ 1 mod 60 ,

Antwort: (Zahlen eintragen)
Entspechend der linearen Kongruenz ist eine Gleichung der obigen Form nur dann für d lösbar, wenn der ggT(_____)=1.

Weiters liefert der erweiterte Euklidische Algorithmus zum ggT(_____) eine Linearkombination der folgenden Art:
ggT(_____) = k* _____ + d* _____

Berechnung von d mit dem erweiterten eukl. Algorithmus:

ggT berechnen	division	modulo	Linearkombination	Rest
ggT(60,17)				
				rückwärts einsetzen
				k= _____ d= _____

Um d positiv zu erhalten, kann man -wegen der Restklasse mod 60– zu d 1*60 oder 2*60 … addieren.

Somit ist d= _____ eine Lösung. **Probe: (17*_____) mod 60 = 1**

1.3. Aufgabe2: Ver/Entschlüsseln, Signieren/Verifizieren

Zeigen Sie das RSA Verfahren, indem Sie den Text ADE in der Tabelle unten -unter Verwendung der folg. Schlüsseln- ver/entschlüsseln bzw. signieren/verifizieren. Um hier einfacher rechnen zu können, verwenden Sie folg. Kodierung der Zeichen: (A → 1, B → 2, ...)

(5 , 91) = (e,n) .... public key **(29, 91) = (d,n) .... private Key**
http://web2.0rechner.de/

m (Buchst.)	**A**	**D**	**E**
m (kodiert)	1		
c (verschlüsselt) c= _____			
s (signiert) s= _____			
m (verifizieren) m= s_____			
m (entschlüsseln) m= c_____			

1.4. Aufgabe: Alice:verschlüsselt→ Bob: signiert → Ted:verifiziert

1. Alice schickt einen verschlüsselten Text an Bob.
2. Bob entschlüsselt diesen Text und sendet ihn signiert an Ted.
3. Ted verifiziert den Text.

Aufgabe: Tragen Sie unten jeweils ein, was wer zu tun hat.

Alice: verschlüsselt →	Bob: signiert →	Ted: verifiziert