CSS 2 Hausübung

Quang Duy Nguyen, Egemen Ulutürk, Leonard Bongard, Ganesha Welsch

1)

a)

- x probieren: Y^x => 3^5 = 9
- y probieren: X^y => 2^8 = 9
  Key = 9

b)

x = g * a: Das Problem ist, dass wir mit unseren Infos, einfach die Formel umstellen können und so auch einfach errechnen können.

2)

Vorgehensweise: Jede Möglichkeit nochmal verschlüsselt und dann auf Gleichheit mit den vorgegebenen Verschlüsselten Nachrichten verglichen.

- Alice: 1,7
- (Bob: 2,3)
- (Charlie: 4,0)

3)

a)

Enc(77,5) = 71

Enc(77,6)=71

b)

Beide Verschlüsselungen haben das gleiche Ergebnis.

Dieses Ergebnis entsteht, da es nur 77 Äquivalenzklassen gibt. Also wird die (und damit jede) Äquivalenzklasse Unendlich oft aufgerufen.

c)

p = 53; q= 59

phi(N)=(p-1)*(q-1) = (53-1)*(59-1) = 3016

e muss Teilerfremd zu 3016 sein. → ggT(3016,6) = 2← Bedingung verletzt

ggT(3016,7) = 1 →erw. Eukl. Algo. K = -1 und L = 431

also ist der Private Key sk(3127,431)