Post'sches Korrespondenzproblem

Ziel: Es sollen Wörter verschlüsselt werden, dabei darf es nicht passieren, dass 2 verschiedene Wörter dieselbe Verschlüsselung erhalten.

windows xp ohne sp: kennwörter mit mehr als 10 buchstaben lassen sich nicht mehr ändern, weil sie identische Hash-Werte besitzen

Frage: Gibt es unterschiedliche Kodierungen, dass es Wörter gibt, die in beiden Kodierungen gleich heißen?

Beispiel:

Klartext	Code α	Code β
a	1	111
b	10111	10
c	10	0

baac ist in α 10111 1 1 10 und in β 10 111 111 0

Man suche weitere, gibt es kürzere?, man beweise, dass es keine 1-buchstabigen, 2-buchstabigen geben kann.

Man beweise, dass es für

Klartext	Code α	Code β
a	10	101
b	011	11
c	101	011

kein Wort gibt, dass in beiden Codes gleich verschlüsselt wird.

Das kürzeste Wort aus {a,b,c,d} , das in beiden Codes gleich verschlüsselt wird hat 44 Buchstaben

Klartext	Code α	Code β
a	0	1
b	01	0
c	1	101

Man schreibe ein Programm, Prolog oder Pascal, das dies findet, wobei man vorher nicht weiß, dass es 44 Buchstaben sind.

Man schaue http://www.theory.informatik.uni-kassel.de/~stamer/pcp/