CS-480 Homework 3

Kevin Argumedo

1. Nibbles: 1001 1111 0100 0010 ;

W0 = 9F; w1 = 42; w2 = B2; w3=F0; w4=D1; w5=63;

k0=9F42; k1=B2F0; k2=15E5

T2=RotWord(w1)=24🡪subword(24)=AD; T2 = AD⊕RC[1]=AD⊕80=2D;

W2 = 2D⊕9F=B2; w3=B2⊕42=F0;

T4=Rotword(F0)=0F🡪subword(0F)=93; T4=93⊕RC[2]=93⊕30=A7;

W4=A7⊕B2=15; w5=15⊕F0=E5;

1. 15116060 mod 53=(1552)2,230\*1548 mod 53 = 1 \* 1548 mod 53 = 13 mod 53
2. 49^-1 mod 416; 49φ(416)-1 mod 416 = 49191mod 416 = 17 mod 416.

C) 101^-1 mod 598; 101φ(598)-1 mod 598 = 101264-1 mod 598 = 225 mod 598

D) 97-1 mod 1056 = 97φ(1056)-1 mod 1056 = 97319  mod 1056 = ­577 mod 1056

E)

1. Alice and Bob will create their Keys using p = 101 and q = 211.

n = pxq= 21311, ø(n) = (p-1)(q-1) = 21000. e = 31; GCD(21311, 31) = 1;

d = e-1 mod ø(n) = 12871; Bob gets privkey(d, n). Alice gets pubkey(e,n);

1. Alice encrypts P using the pubkey. C = 11331 mod 21311 = 2123.

Bob decrypts C: 212312871 mod 21311 = 113;

1. If Bob wants to send Alice something, he needs to get her public key.(slide 12-20. New keys will be made.). P=269; Q=271; n = 72899; ø(n) = 72360; e = 29; d = 57389;

Bob will send to Alice by using his pub key(29, 72899);

C = 11329 mod 72899 = 52000.

Alice will decrypt with privkey: 5200057389 mod 72899 = 113

1. If Alice wants to send P=113 to Bob, then she Digests(D) P(113) and encrypts it with D31 mod 21311. She will send Bob the signature and the message in the same file. When bob receives the message, he will decrypt the digest with M12871 mod 21311. He will be able to get the original digest. He will then digest the message he received and compare the digest he unencrypted with the digest he created with the message.
2. If Bob wants to send P=113 to Alice, he will Digest P = 113 and encrypt it with D29 mod 72899. He will send both the signature and the message in the same file. When Alice receives it, she will decrypt the digest with M57389 mod 72899. (her keys) She will get the original digest and then digest the message and compare to digests to make sure the file was not tampered with.
3. A) P=1327, e1 =5; d= 512; r = 103; e2 = 5512 mod 1327 = 1117;

C1 = 5103mod1327 = 1298;

Pairs: (1298,1247),(1298,405),(1298,810),(1298,373),(1298,421)

(P) C2= (15\*1117103mod1327 = 1247;

(H) C2= (07\*1117103mod1327 = 405;

(O) C2= (14\*1117103mod1327 = 810;

(N) C2= (13\*1117103mod1327 = 373;

(E) C2= (04\*1117103mod1327 = 421;

1. Decrypt with P=C2 \* C1p-1-d mod p;

(1298, 421) ; P=421\*12981327-1-512 mod 1327 = 04 = E;

(1298, 874) ; P=874\*12981327-1-512 mod 1327 = 02 = C;

(1298, 1231);P=1231\*12981327-1-512 mod 1327 =18 = S;

(1298, 341) ; P=341\*12981327-1-512 mod 1327 = 20 = T;

1. A) p = 43; q =31; n=1333; GCD(1333,28)=1;C=p2 mod n= 282 mod 1333= 784
2. A) P= 881; e1 = 3; d = 61; r = 7; M = 300;

E2 = 361 mod 881 = 589;

S1=37mod 881 = 425;

S2= (300-61(425))7-1 mod 880 = -25625\*503 mod 880 = 865;

1. V1 = e1M = 3300 mod 881 = 102;

V2 = e2s1\*S­1s2= 589425\*425865 mod 881 = 102

1. P=787; q = 131; d =57; r=17;

e0=5; e1=5786/131mod 787=672; e2=67257mod 787 = 779

A)S1= (67217 mod 787) mod 131 = 62;

S2 = (100 + 57(62))\*54 mod 131 = 129

1. You verify by finding S2-1 = 96;

V = (672120\*96\*77957\*96 mod 787) mod 131 = 113.

S1=57 ≠ V = 113. The signature does not match.

1. Alice priv= 45; Bobs priv = 27; g = 11; p = 983;

R1 = 1145 mod 983 = 197; R2= 1127 983 = 549;

1. Alice gets R2 from Bob and uses R245 mod 983 = shared key = 358;
2. Bob gets R1 from Alice and uses R127 mod 983 = shared key = 358;