CSS441 – Public Key Cryptography Notes

RSA Key Generation:

$p = 13 \quad , \quad q = 23$

$n = pq$
$= 13 \times 23$
$= 299$

$\phi(n) = \phi(pq)$
$= \phi(p)\phi(q)$
$= \phi(13) \times \phi(23)$
$= 12 \times 22$
$= 264$

$e = 5 \qquad \gcd(264, 5) = 1$

$e \times d \bmod \phi(n) = 1$

$5 \times \underline{53} \bmod 264 = 1$

$d = 53$

$PU_A = (e = 5, n = 299) \qquad PR_A = (\underline{d = 5}3, n = 299)$

$\underline{p = 13} \quad \underline{q = 23} \quad \underline{\phi(n) = 264}$

Figure 1: RSA Key Generation Example 1; Lecture 12

User B: $p = 17$, $q = 11$ $n = 17 \times 11$
$= 187$

$\phi(187) = \phi(17 \times 11)$
$= 16 \times 10$
$= 160$

$\gcd(e, 160) = 1$ $3, 7, 9, \ldots$

$e = 3$ $\_ \times 3 \bmod 160 = 1$
$d = 107$ $161 \div 3$ x
$321 \div 3 = 107$

$e = 7$, $d = 23$

$PU_B = (e = 7, n = 187)$ $PR_B = (d = 23, n = 187)$

Figure 2: RSA Key Generation Example 2; Lecture 12

User A

$PU_A = (e=5, n=299)$

$PR_A = (d=53, n=299)$

$PU_B = (e=7, n=187)$

User B

$PU_B = (e=7, n=187)$

$PR_B = (d=23, n=187)$

$PU_A = (e=5, n=299)$

$M = 8$

$C = M^e \bmod n$

$= 8^7 \bmod 187$

$= 134$

$\xrightarrow{C=134}$

Attacker

$M = C^d \bmod n$

$= 134^{23} \bmod 187$

$= 8$

Known by attacker: $C = 134$

$PU_B = (e=7, n=187)$

Find M, d ??

1 Try M ? $C = M^e \bmod n$

$134 = M^7 \bmod 187$

Practice : not possible if n is large

2 Inverse M ? $7 = \mathrm{dlog}_{M,187}(134)$

Practice : dlog( ) not possible

3 $M = \underline{C}^d \bmod \underline{n}$

$e \times d \bmod \phi(n) = 1$

$7 \times d \bmod \phi(187) = 1$

Manual : $\phi(n)$ is not possible

Factor n into p,q : not possible

Figure 3: RSA Encryption for Confidentiality; Lecture 12

RSA $\quad C = M^e \bmod n$

$$M = C^d \bmod n$$

Probable Message Attack:

Try all possible M:

$$C_1 = M_1^e \bmod n \qquad C_1 \neq C$$
$$C_2 = M_2^e \bmod n \qquad C_2 \neq C$$
$$\vdots$$
$$C_x = M_x^e \bmod n \qquad C_x = C$$

Figure 4: RSA Probable Message Attack; Lecture 13

RSA Enc. $C = M^e \bmod n$

RSA Dec. $M = C^d \bmod n$

$M=5, \; e=17, \; d=4, \; n=21$

$C = 5^{17} \bmod 21$

$= 17$

$M' = 17^4 \bmod 21$

$= 4$ $\quad M' \neq M$

$M' = C^d \bmod n$

$= (M^e \bmod n)^d \bmod n$

$= (M^e)^d \bmod n$

$M' = M^{ed} \bmod n$

When does $M' = M$?

$a = a^{\phi(n)+1} \bmod n$ (Euler's)

When $ed = \phi(n)+1$

$ed \bmod \phi(n) = (\phi(n)+1) \bmod \phi(n)$

$ed \bmod \phi(n) = 1$

$MI(d) = e \quad (\bmod \phi(n))$

$e, \phi(n)$ are relatively prime

$n = p \times q \quad \phi(n) = (p-1) \times (q-1)$

Figure 5: Proof of RSA Encryption Success; Lecture 13

A	B
$q = 353$	$q = 353$
$\alpha = 3$	$\alpha = 3$

$X_A = 97$

$Y_A = \alpha^{X_A} \bmod q$

$= 3^{97} \bmod 353$

$= 40$

$\xrightarrow{Y_A = 40,\ \alpha = 3,\ q = 353}$ $X_B = 233$

$Y_B = \alpha^{X_B} \bmod q$

$= 3^{233} \bmod 353$

$= 248$

$\xleftarrow{Y_B = 248}$

$K_A = Y_B^{X_A} \bmod q$ | $K_B = Y_A^{X_B} \bmod q$

$= 248^{97} \bmod 353$ | $= 40^{233} \bmod 353$

$= 160$ | $= 160$

Shared secret $K = 160$

Attacker Knows: $q = 353,\ \alpha = 3,\ Y_A = 40,\ Y_B = 248$

$K_A = Y_B^{X_A} \bmod q$

$= 248^{X_A} \bmod 353$

$Y_A = \alpha^{X_A} \bmod q$

$40 = 3^{X_A} \bmod 353$

$X_A = \mathrm{dlog}_{3,353}(40)$

Figure 6: Diffie-Hellman Key Exchange Example 1; Lecture 14

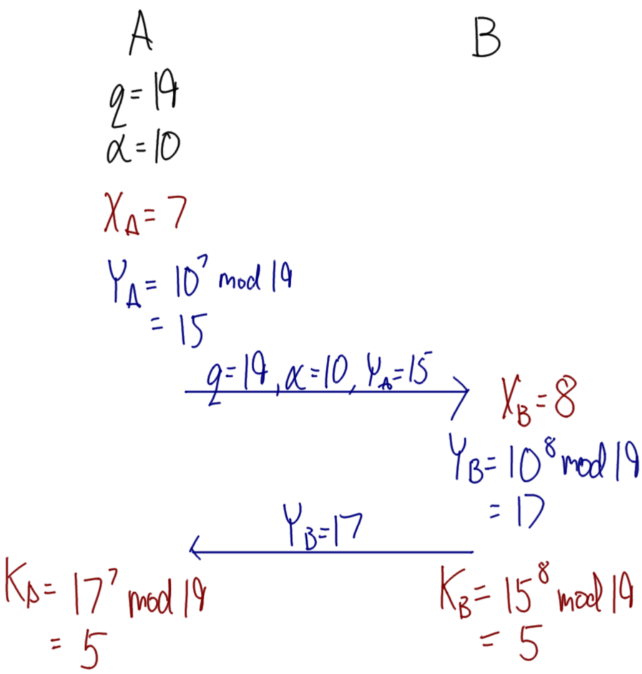

Figure 7: Diffie-Hellman Key Exchange Example 2; Lecture 14

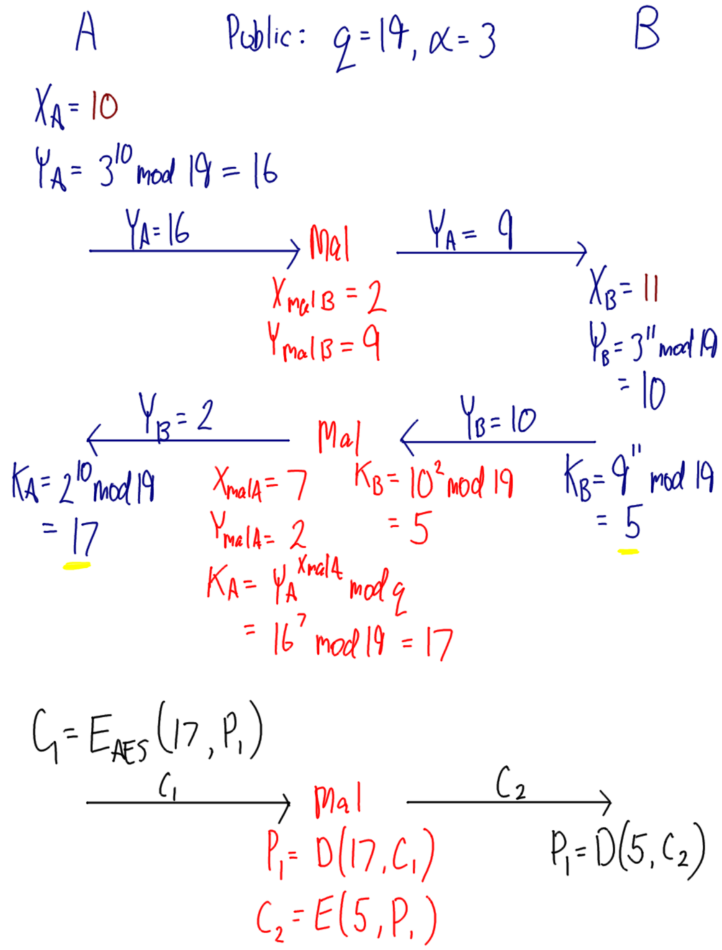

Figure 8: Man-in-the-middle attack on Diffie-Hellman; Lecture 15