ITS335 – Public Key Cryptography Notes

RSA Key Generation:

$p = 17$ $\quad q = 11$

$n = p \times q$

$= 187$ ← public

$\phi(n) = \phi(p) \times \phi(q)$

$= (p-1) \times (q-1)$

$= 16 \times 10$

$= 160$

$e: \quad \gcd(e, \phi(n)) = 1, \; 1 < e < \phi(n)$

$\cancel{2}\ 3\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ \cancel{8}\ 9\ \cancel{10}\ 11 \ldots$

↑

$e = 7$ ← public

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

$7 \times \_ \bmod 160 = 1$

$7 \times 23 = 161$

$7 \times \_ = 321$

$7 \times \_ = 481$

$\vdots$

$d = 23$

$PU_A = (e = 7, n = 187)$ $\quad PR_A = (d = 23, n = 187)$

Figure 1: RSA Key Generation 1; Lecture 12

Key generation:

$p = 13, \quad q = 23$

$n = 13 \times 23 = 299$

$\phi(299) = 12 \times 22 = 264$

e : $\gcd(e, 264) = 1$

$e = 5$ $\qquad e = 7$

$d = 53$ $\qquad d = 151$

Why? $5 \times 53 \bmod 264 = 1$

$PU_B = (e=5, n=299) \quad PR_B = (d=53, n=299)$

Figure 2: RSA Key Generation 2; Lecture 12

A

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

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

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

B

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

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

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

Confidential message $A \to B$ $\quad M = 15$

$C = E(PU_B, M)$

$= M^e \bmod n$

$= 15^5 \bmod 299$

$= 214 \xrightarrow[C=214]{} M' = D(PR_B, C)$

$= C^d \bmod n$

$= 214^{53} \bmod 299$

$= 15$

Figure 3: RSA Encryption; Lecture 12

Attacker: $C = 214$, $PU_B = (e = 5, n = 299)$

$C = M^e \bmod n$

$214 = M^5 \bmod 299$

① Try all M: make M large

make n large

② $\mathrm{dlog}_{m,299}(214) = 5$

$M = C^d \bmod n$

$m = 214^d \bmod 299$

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

$5 \times d \bmod \phi(299) = 1$

Find $\phi(n)$: - factor into p, q

- manually solve $\phi(n)$

Figure 4: RSA Attach Methods; Lecture 12

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

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

When does $M = M'$?

$M = 5 \quad e = 17 \quad d = 4 \quad n = 20$

Enc. $C = 5^{17} \bmod 20$
$= 5$

Dec. $M' = 5^4 \bmod 20$
$= 5$

$M = 5 \quad e = 17 \quad d = 4 \quad n = 21$

$C = 17$

$M' = 4$ X

$$M' = C^d \bmod n$$
$$= (M^e \bmod n)^d \bmod n$$
$$= (M^e)^d \bmod n$$
$$M' = M^{ed} \bmod n$$
$$M = M^{ed} \bmod n$$
$$a = a^{\phi(n)+1} \bmod n \quad \text{(Euler's)}$$

$$ed = \phi(n) + 1$$
$$ed \bmod \phi(n) = 1$$
$$MI(d) = e \quad (\bmod \phi(n))$$

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

p, q: $n = p \times q$

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

Figure 5: Proof that RSA Encrypt Works; Lecture 12

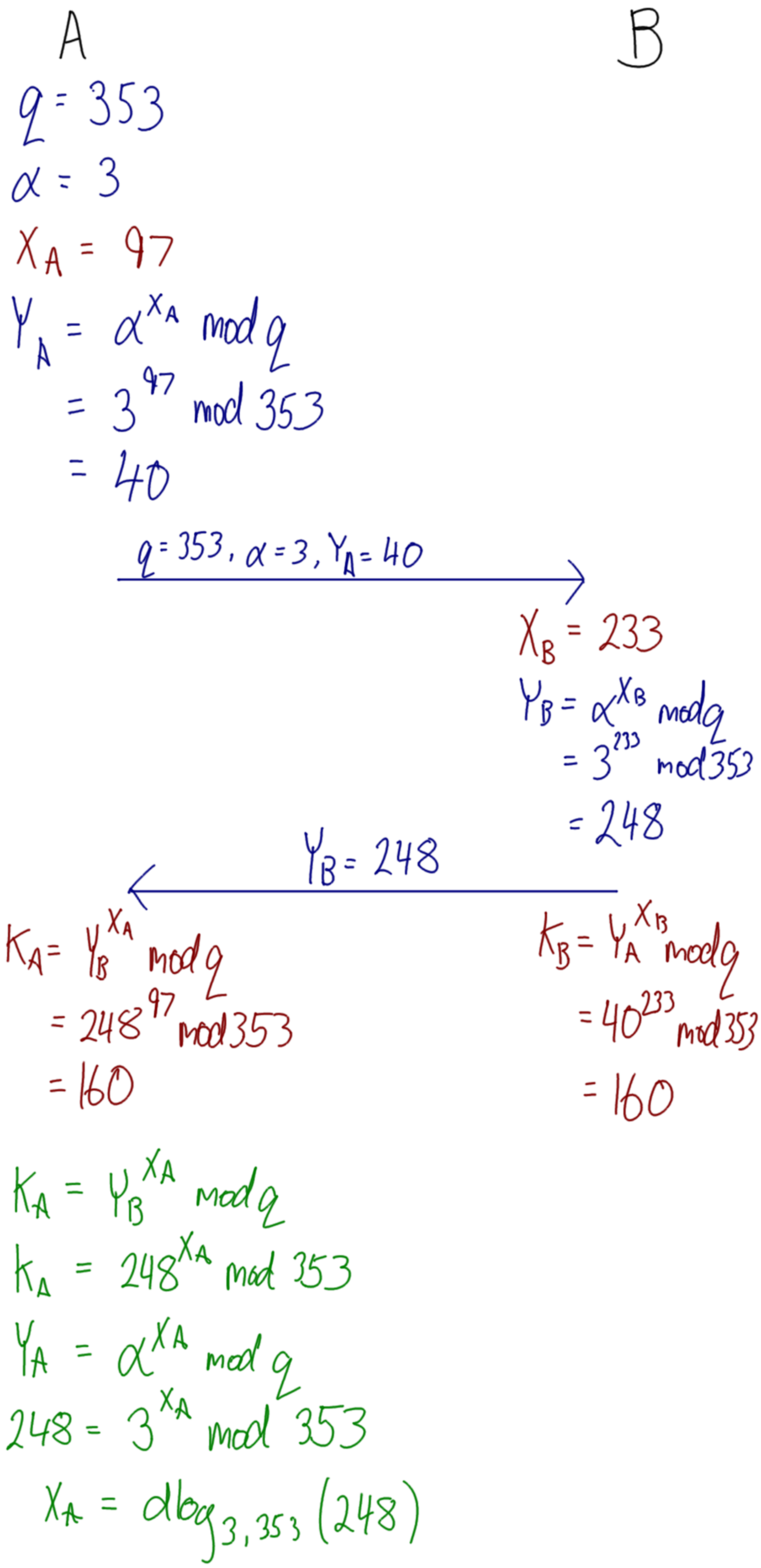

Figure 6: Diffie-Hellman Example 1; Lecture 15

A

$q = 19$

$\alpha = 10$

$X_A = 7$

$Y_A = 10^7 \bmod 19$

$= 15$

$\xrightarrow{q=19,\ \alpha=10,\ Y_A=15}$

$X_B = 8$

$Y_B = 17$

$\xleftarrow{Y_B=17}$

$K_A = 17^7 \bmod 19$ $\quad$ $K_B = 15^8 \bmod 19$

$= 5$ $\quad$ shared secret $\quad$ $= 5$

Attacker knows: $q = 19$, $\alpha = 10$, $Y_A = 15$

$Y_B = 17$

Figure 7: Diffie-Hellman Example 2; Lecture 15

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

$$K_A = Y_B^{X_A} \bmod q \qquad K_B = Y_A^{X_B} \bmod q$$
$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \qquad = (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$
$$= (\alpha^{X_B})^{X_A} \bmod q \qquad = (\alpha^{X_A})^{X_B} \bmod q$$
$$= \alpha^{X_B X_A} \bmod q \qquad = \alpha^{X_A X_B} \bmod q$$

Figure 8: Proof of Diffie-Hellman Key Exchange; Lecture 15

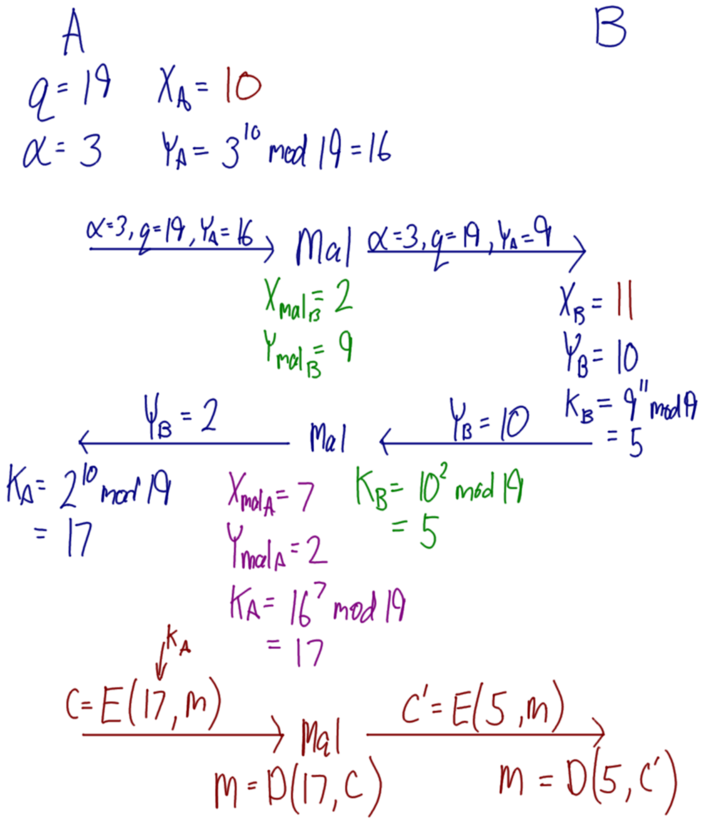

Figure 9: Diffie-Hellman Man-in-the-Middle Attack; Lecture 15