RSA Chosen Ciphertext Attack

RSA CCA

- Eve intercepts Ciphertext C sent from Alice to Bob as Eve is interested in the corresponding plaintext M.
  - We have $C = M^e \bmod n$
- Now Eve **chooses** another ciphertext C' to send to Bob such that Bob decrypts it and sends the message back to Eve.
  - $C' = C \times r^e \bmod n$
  - r is a random number chosen such that gcd(n,r)=1
  - Bob decrypts C' as Y= $(C')^d \bmod n$
- Eve gets Y and then determine the plaintext M because:
  - Y= $(C \times r^e)^d \bmod n$
  - Y= $(M^e \times r^e)^d \bmod n$
  - Y= $M \times r \bmod n$ Since ed are inverses
  - Y, r and n are known and required to know M
  - M= $Y \times r^{-1} \bmod n$
  - Use Extended Euclidean algorithm to find r^{-1}

Extended Euclidean Algorithm

- For given integers a and b , the extended Euclidean algorithm not only calculate the greatest common divisor but also two additional integers x and y that satisfy the following equation:

$$ax + by = d = \gcd(a, b)$$

- It should be clear that x and y will have opposite signs.
- Useful for later crypto computations
- follow sequence of divisions for GCD but assume at each step i, can find x &y: r = ax + by at end find GCD value and also x & y
- More generally, the extended Euclidean algorithm can be used to find a multiplicative inverse in Z_n for any n. If we apply the extended Euclidean algorithm to the equation $nx + by = d$, and the algorithm yields $d = 1$, then $y = b^{-1}$ in Z_n.

Extended Euclidean Algorithm

Extended Euclidean Algorithm			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
• • •	• • •	• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-1} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_n \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

Extended Euclidean Algorithm: Example

$a = 1759$ $b = 550$

Table 4.4 Extended Euclidean Algorithm Example

i	r_i	q_i	x_i	y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: $d = 1$; $x = -111$; $y = 355$

Thus, $b^{-1} = 355$.

Thank You