Attacking RSA Web Lesson

Start the audio player below to begin the lesson

(1) 00:43 Suppose Alice's public key is $(1363, 671)$ and Bob's public key is $(989, 523)$. Bob sends ciphertext 644 to Alice. What is the plaintext?

(2) 01:20 Let P be the plaintext. Bob used Alice's public key to compute the ciphertext.

Bob: $P^{671} \pmod{1363} = 644 \pmod{1363}$

(3) 02:15 To determine P, we need Alice's private key $(1363, m)$. Then $644^m \pmod{1363} = P \pmod{1363}$.

(4) 02:53 To determine m, we first need to factor 1363. Trial division and Fermat's factorization method both require 9 steps.

$\sqrt{1363 + 9^2} = 38$ $\qquad$ $1363 = (38-9)(38+9) = 29 \cdot 47$

(5) 04:09 Now compute $\phi(1363)$.

$\phi(1363) = (29-1)(47-1) = 1288$

(6) 04:33 Since Alice's public key is $(1363, 671)$, then $m = 671^{-1}$ in $\mathbb{Z}_{1288}$. We use the extended Euclidean algorithm to find m.

(7) 05:02 First use the Euclidean algorithm to find $\gcd(1288, 671)$. The result should be 1 (else 671^{-1} does not exist in $\mathbb{Z}_{1288}$).

(8) 05:46

$$1288 = 1 \cdot 671 + 617 \qquad 1 \cdot \underline{1288} - 1 \cdot \underline{671} = 617$$
$$671 = 1 \cdot 617 + 54 \qquad 1 \cdot \underline{671} - 1 \cdot \underline{617} = 54$$
$$617 = 11 \cdot 54 + 23 \qquad 1 \cdot \underline{617} - 11 \cdot \underline{54} = 23$$
$$54 = 2 \cdot 23 + 8 \qquad 1 \cdot \underline{54} - 2 \cdot \underline{23} = 8$$
$$23 = 2 \cdot 8 + 7 \qquad 1 \cdot \underline{23} - 2 \cdot \underline{8} = 7$$
$$8 = 1 \cdot 7 + 1 \qquad 1 \cdot \underline{8} - 1 \cdot \underline{7} = 1$$

(9) 06:31

Now find 671^{-1} in $\mathbb{Z}_{1288}$ by using the equations on the right in (8).

$$1 \cdot \underline{8} - 1 \cdot \underline{7} = 1 \qquad 1 \cdot \underline{8} - 1(1 \cdot \underline{23} - 2 \cdot \underline{8}) = 1$$
$$-1 \cdot \underline{23} + 3 \cdot \underline{8} = 1 \qquad -1 \cdot \underline{23} + 3(1 \cdot \underline{54} - 2 \cdot \underline{23}) = 1$$
$$3 \cdot \underline{54} - 7 \cdot \underline{23} = 1 \qquad 3 \cdot \underline{54} - 7(1 \cdot \underline{617} - 11 \cdot \underline{54}) = 1$$
$$-7 \cdot \underline{617} + 80 \cdot \underline{54} = 1 \qquad -7 \cdot \underline{617} + 80(1 \cdot \underline{671} - 1 \cdot \underline{617}) = 1$$
$$80 \cdot \underline{671} - 87 \cdot \underline{617} = 1 \qquad 80 \cdot \underline{671} - 87(1 \cdot \underline{1288} - 1 \cdot \underline{671}) = 1$$
$$-87 \cdot \underline{1288} + 167 \cdot \underline{671} = 1$$

(10) 07:46

$$-87 \cdot \underline{1288} + 167 \cdot \underline{671} = 1$$

The above equation tells use that $671^{-1} = 167$ in $\mathbb{Z}_{1288}$.

Alice's private key: $(1363, 167)$

(11) 08:39

The ciphertext is 644 and Alice's private key is $(1363, 167)$. So $P \pmod{1363} = 644^{167} \pmod{1363}$, we need to compute $644^{167} \pmod{1363}$.

(12) First convert 167_{10} to base-2.

09:07

$167 = 83 \cdot 2 + 1$

$83 = 41 \cdot 2 + 1$

$41 = 20 \cdot 2 + 1$

$20 = 10 \cdot 2 + 0$

$10 = 5 \cdot 2 + 0$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$0 = 0 \cdot 2 + 1$

$167_{10} = 10100111_2$

(13) Replace each 1 in the base-2 representation with 644 and replace each 0 with a 1.

09:53

Mod 1363

	644
$644^2 = 384$	$384 \cdot 1 = 384$
$384^2 = 252$	$252 \cdot 644 = 91$
$91^2 = 103$	$103 \cdot 1 = 103$
$103^2 = 1068$	$1068 \cdot 1 = 1068$
$1068^2 = 1156$	$1156 \cdot 644 = 266$
$266^2 = 1243$	$1243 \cdot 644 = 411$
$411^2 = 1272$	$1272 \cdot 644 = 5$

We see that $644^{167} \pmod{1363} = 5 \pmod{1363}$

(14) The plaintext is 5.

11:28