Public key cryptography

Public key cryptography

For Person A to receive messages...

Step 1: Make a cypher, turning letters into numbers.

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For example, "TO BE OR NOT TO BE" becomes

$$30251215252824253030251215:$$

T	O	B	E	O	R	N	O	T	T	O	B	E
30	25	12	15	25	28	24	25	30	30	25	12	15

(Use a larger key to include spaces and punctuation, etc.)

For Person A to receive messages...

Step 1: Make a cypher, turning letters into numbers.

Step 2: Choose two large primes p and q, and let $n = pq$.

[Generally, chosen randomly, but within a couple of digits in length of each other.]

For Person A to receive messages...

Step 1: Make a cypher, turning letters into numbers.

Step 2: Choose two large primes p and q, and let $n = pq$.

[Generally, chosen randomly, but within a couple of digits in length of each other.]

Ex: Let $p = 12553$, $q = 13007$.

For Person A to receive messages...

Step 1: Make a cypher, turning letters into numbers.

Step 2: Choose two large primes p and q, and let $n = pq$.

[Generally, chosen randomly, but within a couple of digits in length of each other.]

Ex: Let $p = 12553$, $q = 13007$. So $n = 163276871$.

For Person A to receive messages...

Step 1: Make a cypher, turning letters into numbers.

Step 2: Choose two large primes p and q, and let $n = pq$.

[Generally, chosen randomly, but within a couple of digits in length of each other.]

Ex: Let $p = 12553$, $q = 13007$. So $n = 163276871$.

Step 3: Compute $\phi(pq) = (p-1)(q-1)$, and pick a number k relatively prime to $\phi(pq)$.

[Specifically, pick k randomly between 10 and $\mathrm{lcm}(p-1, q-1)$.]

For Person A to receive messages. . .

Step 1: Make a cypher, turning letters into numbers.

Step 2: Choose two large primes p and q, and let $n = pq$.

[Generally, chosen randomly, but within a couple of digits in length of each other.]

Ex: Let $p = 12553$, $q = 13007$. So $n = 163276871$.

Step 3: Compute $\phi(pq) = (p-1)(q-1)$, and pick a number k relatively prime to $\phi(pq)$.

[Specifically, pick k randomly between 10 and $\mathrm{lcm}(p-1, q-1)$.]

Ex: $\phi(n) = 12552 * 13006 = 163251312$.

For Person A to receive messages...

Step 1: Make a cypher, turning letters into numbers.

Step 2: Choose two large primes p and q, and let $n = pq$.

[Generally, chosen randomly, but within a couple of digits in length of each other.]

Ex: Let $p = 12553$, $q = 13007$. So $n = 163276871$.

Step 3: Compute $\phi(pq) = (p-1)(q-1)$, and pick a number k relatively prime to $\phi(pq)$.

[Specifically, pick k randomly between 10 and $\mathrm{lcm}(p-1, q-1)$.]

Ex: $\phi(n) = 12552 * 13006 = 163251312$. Pick $k = 79921$.

For Person A to receive messages. . .

Step 1: Make a cypher, turning letters into numbers.

Step 2: Choose two large primes p and q, and let $n = pq$.

[Generally, chosen randomly, but within a couple of digits in length of each other.]

Ex: Let $p = 12553$, $q = 13007$. So $n = 163276871$.

Step 3: Compute $\phi(pq) = (p-1)(q-1)$, and pick a number k relatively prime to $\phi(pq)$.

[Specifically, pick k randomly between 10 and $\mathrm{lcm}(p-1, q-1)$.]

Ex: $\phi(n) = 12552 * 13006 = 163251312$. Pick $k = 79921$.

Step 4: Publish the cypher, n, and k publicly; keep p, q, and $\phi(pq)$ secret.

Published: $n = 163276871$, $k = 79921$, and cypher

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For Person B to send messages...

Published: $n = 163276871$, $k = 79921$, and cypher

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For Person B to send messages...

Step 1: Using the provided cypher, turn letters into numbers, and break into small-ish pieces (fewer digits than n).

Published: $n = 163276871$, $k = 79921$, and cypher

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For Person B to send messages...

Step 1: Using the provided cypher, turn letters into numbers, and break into small-ish pieces (fewer digits than n).

Ex: TO BE OR NOT TO BE → $30251215252824253030251215$

$$a_1 = 30251215, \quad a_2 = 25282425, \quad a_3 = 30302512, \quad a_4 = 15.$$

Published: $n = 163276871$, $k = 79921$, and cypher

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For Person B to send messages...

Step 1: Using the provided cypher, turn letters into numbers, and break into small-ish pieces (fewer digits than n).

Ex: TO BE OR NOT TO BE $\rightarrow$ $302512152528242530302512 15$

$$a_1 = 30251215, \quad a_2 = 25282425, \quad a_3 = 30302512, \quad a_4 = 15.$$

Step 2: Compute $a_i^k \pmod{n}$ for each piece.

Published: $n = 163276871$, $k = 79921$, and cypher

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For Person B to send messages. . .

Step 1: Using the provided cypher, turn letters into numbers, and break into small-ish pieces (fewer digits than n).

Ex: TO BE OR NOT TO BE → 30251215252824253030251215

$$a_1 = 30251215, \quad a_2 = 25282425, \quad a_3 = 30302512, \quad a_4 = 15.$$

Step 2: Compute $a_i^k \pmod{n}$ for each piece.

Ex:

$$30251215^{79921} \equiv_{163276871} 149419241$$
$$25282425^{79921} \equiv_{163276871} 62721998$$
$$30302512^{79921} \equiv_{163276871} 118084566$$
$$15^{79921} \equiv_{163276871} 40481382$$

Published: $n = 163276871$, $k = 79921$, and cypher

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For Person B to send messages...

Step 1: Using the provided cypher, turn letters into numbers, and break into small-ish pieces (fewer digits than n).

Ex: TO BE OR NOT TO BE → $30251215252824253030251215$

$$a_1 = 30251215, \quad a_2 = 25282425, \quad a_3 = 30302512, \quad a_4 = 15.$$

Step 2: Compute $a_i^k \pmod{n}$ for each piece.

Ex:

$$30251215^{79921} \equiv_{163276871} 149419241$$
$$25282425^{79921} \equiv_{163276871} 62721998$$
$$30302512^{79921} \equiv_{163276871} 118084566$$
$$15^{79921} \equiv_{163276871} 40481382$$

Step 3: Send the results.

Back to Person A: You know $n = 163276871$, $k = 79921$, and the cypher. You *also* know $p = 12553$ and $q = 13007$, so that $\phi(n) = 163251312$.

Back to Person A: You know $n = 163276871$, $k = 79921$, and the cypher. You *also* know $p = 12553$ and $q = 13007$, so that $\phi(n) = 163251312$. So now, given that

$$a_1^k \equiv_n 149419241, \quad a_2^k \equiv_n 62721998,$$
$$a_3^k \equiv_n 118084566, \quad \text{and} \quad a_4^k \equiv_n 40481382,$$

you can use the methods from last time to solve for a_1, a_2, a_3, and a_4!

Back to Person A: You know $n = 163276871$, $k = 79921$, and the cypher. You *also* know $p = 12553$ and $q = 13007$, so that $\phi(n) = 163251312$. So now, given that

$$a_1^k \equiv_n 149419241, \quad a_2^k \equiv_n 62721998,$$
$$a_3^k \equiv_n 118084566, \quad \text{and} \quad a_4^k \equiv_n 40481382,$$

you can use the methods from last time to solve for a_1, a_2, a_3, and a_4! Namely, you use the Euclidean algorithm to compute

$$1 = 145604785 \cdot k - 71282 \cdot \phi(n).$$

Back to Person A: You know $n = 163276871$, $k = 79921$, and the cypher. You *also* know $p = 12553$ and $q = 13007$, so that $\phi(n) = 163251312$. So now, given that

$$a_1^k \equiv_n 149419241, \quad a_2^k \equiv_n 62721998,$$
$$a_3^k \equiv_n 118084566, \quad \text{and} \quad a_4^k \equiv_n 40481382,$$

you can use the methods from last time to solve for a_1, a_2, a_3, and a_4! Namely, you use the Euclidean algorithm to compute

$$1 = 145604785 \cdot k - 71282 \cdot \phi(n).$$

Then, you know if $a^k \equiv_n b$, then $a \equiv_n b^u$, where $u = 145604785$.

Back to Person A: You know $n = 163276871$, $k = 79921$, and the cypher. You *also* know $p = 12553$ and $q = 13007$, so that $\phi(n) = 163251312$. So now, given that

$$a_1^k \equiv_n 149419241, \quad a_2^k \equiv_n 62721998,$$
$$a_3^k \equiv_n 118084566, \quad \text{and} \quad a_4^k \equiv_n 40481382,$$

you can use the methods from last time to solve for a_1, a_2, a_3, and a_4! Namely, you use the Euclidean algorithm to compute

$$1 = 145604785 \cdot k - 71282 \cdot \phi(n).$$

Then, you know if $a^k \equiv_n b$, then $a \equiv_n b^u$, where $u = 145604785$. So, using the method of successive squaring, you are able to compute

$$a_1 \equiv 149419241^{145604785} \equiv 30251215 \pmod{163276871},$$
$$a_2 \equiv 62721998^{145604785} \equiv 25282425 \pmod{163276871},$$
$$a_3 \equiv 118084566^{145604785} \equiv 30302512 \pmod{163276871},$$
$$a_4 \equiv 40481382^{145604785} \equiv 15 \pmod{163276871},$$

as desired.

Back to Person A: You know $n = 163276871$, $k = 79921$, and the cypher. You *also* know $p = 12553$ and $q = 13007$, so that $\phi(n) = 163251312$. So now, given that

$$a_1^k \equiv_n 149419241, \quad a_2^k \equiv_n 62721998,$$
$$a_3^k \equiv_n 118084566, \quad \text{and} \quad a_4^k \equiv_n 40481382,$$

you can use the methods from last time to solve for a_1, a_2, a_3, and a_4! Namely, you use the Euclidean algorithm to compute

$$1 = 145604785 \cdot k - 71282 \cdot \phi(n).$$

Then, you know if $a^k \equiv_n b$, then $a \equiv_n b^u$, where $u = 145604785$. So, using the method of successive squaring, you are able to compute

$$a_1 \equiv 149419241^{145604785} \equiv 30251215 \pmod{163276871},$$
$$a_2 \equiv 62721998^{145604785} \equiv 25282425 \pmod{163276871},$$
$$a_3 \equiv 118084566^{145604785} \equiv 30302512 \pmod{163276871},$$
$$a_4 \equiv 40481382^{145604785} \equiv 15 \pmod{163276871},$$

as desired.

RSA public key cryptosystem, after Ron Rivest, Adi Shamir, and Leonard Adleman.