

SSL, private key and public key decoding task

Instructions

- Print out a copy of this document
- Cut out each of the sections
- In pairs, students work to decode the message they have been given
- When they have decoded their message students need to help reassemble all of the messages in the correct order, perhaps using blu-tack and putting them onto a wall, the board or some desks.
- If students decode their message quickly, they can go to help others
- Students should look at the assembled steps and try to understand the process.

You may:

- Guide teachers or students to access this resource from the teach-ict.com site
- Print out enough copies to use during the lesson

You may not:

- Adapt or build on this work
- Save this resource to a school network or VLE
- Republish this resource on the internet

A subscription will enable you to access an editable version and save it on your protected network or VLE

Step 4

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11				15										6	5				10						

T E E E P A E E E E
 10 4 15 21 15 19 2 16 15 5 11 20 15 22 21 2 21 22 7 20 21 15 19 2 16 15
O E T A E () P O T O O
 21 6 19 9 15 10 12 11 8 15 16 21 21 12 5 16 6 10 6 19 6 12 21
(E) A T E T O E A
 16 2 12 15 21 11 7 18 10 4 15 19 2 21 10 6 23 15 16 19 11 7
E E A E E T E T E E
 1 15 15 12 21 11 1 15 15 7 10 15 16 22 7 20 10 4 15 22 16 19 16 15 18 22
T A E T A
 10 19 11 16 18 18 15 10 11 22 12 21

Step 5

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
26				18										10	17				4						

T E T O E E T E T E
 4 20 18 13 2 21 4 10 5 18 15 18 14 4 18 15 21 4 20 18 1 15
E T A E T A A T E
 13 15 18 6 1 4 13 26 15 6 6 18 4 26 1 7 21 26 14 6 4 20 18 1 15
P E O A O A T O T O
 17 18 15 21 10 14 26 7 1 14 23 10 15 5 26 4 1 10 14 1 14 4 10
T E E O
 4 20 18 9 18 24 23 10 15 5

Step 6

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
21				14										20	16				25						

T E O A T O E T E E
 25 10 14 6 5 7 20 19 8 21 25 6 20 5 14 5 25 14 19 14 26 18 11
T E T O E A ' T E T E E
 25 10 14 15 17 24 25 20 8 14 19 10 21 24 5 25 11 14 25 18 14 14 5
E P T E . A T T T A E
 14 5 15 19 11 16 25 14 26 21 25 25 10 6 24 24 25 21 1 14
T A E ' P A T E T '
 6 25 6 24 15 21 12 12 14 26 16 12 21 6 5 25 14 2 25

Step 7

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1				13										5	21				20							

E T E T O E E A
 24 2 13 3 20 2 13 7 18 15 20 5 26 13 10 14 15 10 13 1 8 19
 T E P E T E T O E
 20 2 13 19 21 10 13 15 15 20 2 13 15 18 4 26 14 20 5 10 15 13 3 8
 T T O A E A E A
 4 18 20 20 5 3 1 26 13 15 15 1 23 13 18 15 18 1 9 9 19
 A P P E A A P O E
 1 21 21 13 1 10 15 24 2 14 7 2 15 1 19 15 21 10 5 7 13 15 15 14 3 23
 O E
 5 10 8 13 10

Step 8

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
23				12										22	21				3							

E T E ' T O E ' T T O
 18 5 12 13 3 5 12 26 11 9 15 4 3 22 8 7 12 8 9 11 3 3 22 13
 A E E P E E T E
 5 23 26 9 12 12 13 21 8 12 26 26 12 7 3 5 12 26 26 20
 E A E A E T O T E O P
 26 12 13 7 26 23 15 12 26 26 23 6 12 3 22 3 5 12 26 5 22 21
 A O T E P E
 23 26 19 4 13 6 16 22 8 3 5 12 21 11 9 20 4 24 19 12 10
 T O E E T A T O T E T O E
 3 22 9 12 26 12 13 3 9 23 24 19 3 22 3 5 12 24 11 26 3 22 15 12 8

Step 9

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
13				26										9	18				16							

T E O P ' P E E E
 16 24 26 12 24 9 18 12 18 4 15 10 14 11 3 26 23 14 12 25 26 11 26 14 8
 E T E T O E ' T
 26 20 15 23 16 24 26 11 4 12 16 9 7 26 25 12 12 12 10 14 16
 A P P E T O T E ' P A T E T '
 14 12 13 18 18 10 14 26 20 16 9 16 24 26 18 10 13 14 22 16 26 1 16
 T P E T E T O E E A E
 16 23 18 26 20 14 22 15 23 16 24 26 11 4 12 16 9 7 26 25 26 13 25 10 14 26

Step 10:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1				25										20	23				12						

T E P A **T E T** **O T A**
 12 7 25 23 26 1 17 3 12 25 2 12 6 20 3 12 1 17 3 17 3 15
T E **T O E ' P E** **O A A**
 12 7 25 6 11 14 12 20 21 25 9 14 23 25 9 14 20 3 1 26 1 3 8
A A **E T A** **A E E** **P T E**
 18 17 3 1 3 6 17 1 26 8 25 12 1 17 26 14 1 9 25 25 3 6 9 4 23 12 25
T E A E **O A E** **' P E**
 8 12 7 25 4 1 9 25 3 20 24 6 1 26 26 25 8 6 17 23 7 25 9
T E T '
 12 25 2 12

Step 11

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2				26										13	22				1						

T E **T O E ' O E O**
 1 15 26 24 19 11 1 13 17 26 20 11 3 20 13 14 11 26 20 16 13 14
E **T E E** **P T E** **P E**
 11 26 16 21 11 1 15 26 26 16 24 20 5 22 1 26 21 24 9 22 15 26 20
T E T A E O E T E T E E T
 1 26 10 1 11 2 4 26 8 5 13 18 26 20 1 15 26 9 16 1 26 20 16 26 1
T O T E O P
 1 13 1 15 26 11 15 13 22

Step 12

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
22				7										25	23				1						

E E **A E** **E E T O** **T E E**
 7 24 7 20 2 15 9 22 13 26 7 10 6 4 7 10 7 1 25 2 20 1 7 10 13 7
P T T E **E A E , T E E** **P T O**
 23 1 1 9 7 11 7 6 6 22 3 7 1 9 7 7 20 13 10 16 23 1 2 25 20
O E E T A T T E O
 2 6 6 25 6 7 13 18 10 7 1 9 22 1 1 9 7 16 4 25 18 19 14
O T E A E T O E P E T
 20 25 1 17 7 22 17 19 7 1 25 14 7 13 2 23 9 7 10 2 1

Step 13

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12				1										10	23				21						

T E **O T E** **O P ' E E**
 21 20 1 14 14 26 10 17 21 20 1 14 20 10 23 14 14 1 16 24 1 16
E O **E T A T T E** **O P ' E**
 16 1 9 10 5 17 4 14 1 14 21 20 12 21 21 20 1 14 20 10 23 14
P E A E E E T O
 23 2 13 26 4 9 18 1 11 20 12 14 13 1 1 17 2 14 1 22 21 10
E P T T E E A E .
 1 17 9 16 11 23 21 21 20 1 15 1 14 14 12 5 1

Step 14

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4				18										26	23				24						

T E **O P ' E O E E T E**
 24 19 18 1 19 26 23 1 18 3 26 8 8 18 10 3 18 1 6 1 24 18 8
E T E O P ' ' P A T E E
 20 1 18 1 24 19 18 1 19 26 23 1 23 10 25 7 4 24 18 14 18 6
T O E P T T E P E T E T
 24 26 2 18 3 10 6 23 24 24 19 18 3 25 23 19 18 10 24 18 15 24
A T O P A T E T O T A T
 21 4 3 14 25 12 24 26 23 16 4 25 12 24 18 15 24 1 26 24 19 4 24
T A E E T O O .
 25 24 3 4 12 21 18 20 12 2 18 10 1 24 26 26 2
