Lucente Stabile Atkins

Encryption Algorithm

May 04, 2020

Gauss' Generalization of Wilson's Theorem

Wilson proved that, if p is prime:

$$(p-1)! \equiv -1 \mod p$$

Gauss' Generalization of Wilson's Theorem

Wilson proved that, if p is prime:

$$(p-1)! \equiv -1 \mod p$$

Gauss then generalized, if $U(n)$ is cyclic and $\alpha \in U(n)$:

$$\alpha_1 \cdot \alpha_2 \cdot_3 \ldots \alpha_{\phi(n)-1} \equiv -1 \mod n$$

Key Exchange

Diffie Hellman

Quantum key exchange

Spies in a field

Key Exchange

Diffie Hellman

Quantum key exchange

Spies in a field

Or a company can keep their chosen group a secret which means that no key exchange is needed.

Key Exchange

In our example:

$$k = 53$$

Choosing $U(n)$

Since $k = 53$, and $n = p^t$ or $n = 2p^t$,

Choosing $U(n)$

Since $k = 53$, and $n = p^t$ or $n = 2p^t$,

Check:

$$54 = 2 \cdot 3^3 = 2 \cdot p^t$$

Choosing $U(n)$

So we choose our group to be $U(54)$. Recall that the elements of our group are $\alpha_i \in \mathbf{N}$ that are relatively prime with n:

$$\{1, 5, 7, 11, 12, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53\}$$

Encryption

Encrypting the letter G:

Since G is the seventh letter in the alphabet we map G to the seventh element of the group $U(54)$. So $C \mapsto 19$. The sender first multiplies each element up to 7 to obtain the ciphertext:

Encryption

Encrypting the letter G:

Since G is the seventh letter in the alphabet we map G to the seventh element of the group $U(54)$. So $C \mapsto 19$. The sender first multiplies each element up to 7 to obtain the ciphertext:

$$1 \cdot 5 \cdot 7 \cdot \ 11 \cdot 13 \cdot 17 \cdot 19 = 1,616,651 \equiv 17 \mod 54$$

Encryption

Encrypting the letter G:

Since G is the seventh letter in the alphabet we map G to the seventh element of the group $U(54)$. So $C \mapsto 19$. The sender first multiplies each element up to 7 to obtain the ciphertext:

$$1 \cdot 5 \cdot 7 \cdot \ 11 \cdot 13 \cdot 17 \cdot 19 = 1,616,651 \equiv 17 \mod 54$$

17 is the first element of the ciphertext.

Now the sender finds the number of times we find -1 mod n, called Σ, by preforming the following calculations:

Now the sender finds the number of times we find -1 mod n, called Σ, by preforming the following calculations:

$$
\begin{aligned}
17 \cdot 53 &= 901 \mod 54 \equiv 37 \\
37 \cdot 49 &= 1,813 \mod 54 \equiv 31 \\
31 \cdot 47 &= 1,457 \mod 54 \equiv -1 \rightarrow (\text{first } \Sigma) \\
53 \cdot 43 &= 2,279 \mod 54 \equiv 11 \\
11 \cdot 41 &= 451 \mod 54 \equiv 19 \\
19 \cdot 37 &= 703 \mod 54 \equiv 1 \\
1 \cdot 35 &= 35 \mod 54 \equiv 35 \\
35 \cdot 31 &= 1,085 \mod 54 \equiv 5 \\
5 \cdot 29 &= 145 \mod 54 \equiv 37 \\
37 \cdot 25 &= 925 \mod 54 \equiv 7 \\
7 \cdot 23 &= 161 \mod 54 \equiv -1 \rightarrow (\text{second } \Sigma)
\end{aligned}
$$

Now the sender finds the number of times we find -1 mod n, called Σ, by preforming the following calculations:

$$
\begin{aligned}
17 \cdot 53 &= 901 \mod 54 \equiv 37 \\
37 \cdot 49 &= 1,813 \mod 54 \equiv 31 \\
31 \cdot 47 &= 1,457 \mod 54 \equiv -1 \rightarrow (\text{first } \Sigma) \\
53 \cdot 43 &= 2,279 \mod 54 \equiv 11 \\
11 \cdot 41 &= 451 \mod 54 \equiv 19 \\
19 \cdot 37 &= 703 \mod 54 \equiv 1 \\
1 \cdot 35 &= 35 \mod 54 \equiv 35 \\
35 \cdot 31 &= 1,085 \mod 54 \equiv 5 \\
5 \cdot 29 &= 145 \mod 54 \equiv 37 \\
37 \cdot 25 &= 925 \mod 54 \equiv 7 \\
7 \cdot 23 &= 161 \mod 54 \equiv -1 \rightarrow (\text{second } \Sigma)
\end{aligned}
$$

So $\Sigma = 1$

Frame Title

So our ciphertext is $C = (17, 1)$.

Decryption

The receiver decrypts by starting at the largest group element and multiplying in decending order until he finds $\Sigma + 1$ elements congruent to $-1 \mod n$.

Decrypting $C = (17, 1)$:

$$
\begin{aligned}
17 \cdot 53 &= 901 \mod 54 \equiv 37 \\
37 \cdot 49 &= 1,813 \mod 54 \equiv 31 \\
31 \cdot 47 &= 1,457 \mod 54 \equiv -1 \rightarrow (\text{first } \Sigma) \\
53 \cdot 43 &= 2,279 \mod 54 \equiv 11 \\
11 \cdot 41 &= 451 \mod 54 \equiv 19 \\
19 \cdot 37 &= 703 \mod 54 \equiv 1 \\
1 \cdot 35 &= 35 \mod 54 \equiv 35 \\
35 \cdot 31 &= 1,085 \mod 54 \equiv 5 \\
5 \cdot 29 &= 145 \mod 54 \equiv 37 \\
37 \cdot 25 &= 925 \mod 54 \equiv 7 \\
7 \cdot 23 &= 161 \mod 54 \equiv -1 \rightarrow (\text{second } \Sigma)
\end{aligned}
$$

Decrypt

Now the receiver know that every element of $U(n)$ has been multiplied together.

$$\{1, 5, 7, 11, 12, 17, 19] \; [23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53\}$$
$$\text{Sender} \rightarrow \qquad\qquad \leftarrow \textit{Receiver}$$

Decrypt

Now the receiver know that every element of $U(n)$ has been multiplied together.

$$\{1, 5, 7, 11, 12, 17, 19] \; [23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53\}$$
$$\text{Sender} \rightarrow \qquad\qquad \leftarrow \textit{Receiver}$$

$$\alpha \cdot \alpha^1 \cdot \alpha^2 \cdots \alpha^{\phi(n)-1} \equiv -1 \mod n$$

Decrypt

Now the receiver know that every element of $U(n)$ has been multiplied together.

$$\{1, 5, 7, 11, 12, 17, 19] \; [23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53\}$$
$$\text{Sender} \rightarrow \qquad\qquad \leftarrow \textit{Receiver}$$

$$\alpha \cdot \alpha^1 \cdot \alpha^2 \cdots \alpha^{\phi(n)-1} \equiv -1 \mod n$$