

CYBER SECURITY & CRYPTOGRAPHY

INTRODUCTION TO CRYPTOGRAPHY

An overview of the most common cryptographic methods and algorithms.



Ashad Mohamed
Security Researcher

TABLE OF CONTENT

1

Why Crypto matters

Defining what is crypto and what does it matter.

2

Cryptographic Algorithm

Explaining what is different cryptographic algorithm

3

What is Plaintext?

Explaining what is a plaintext string

4

What is Ciphertext?

Explaining what is a ciphertext

5

What is a key?

Explaining what is a key

6

Symmetric Encryption

Explaining what is symmetric encryption

12

Public Key Infrastructure

Explaining what is PKI and its use

11

Man In the Middle Attack

Showing how can DH be vulnerable to mitm attack

10

Diffie-Hellman Key Exchange

Explaining what DH key exchange and how it works

9

RSA Mathematical Representation

Providing how RSA works.

8

RSA Algorithm

Explaining what is RSA algorithm

7

Asymmetric Encryption

Explaining What is Asymmetric encryption

13

What is Hashing?

Explaining what hashing and its various uses.

14

Prepending the Salt

Giving salting examples

15

Appending the Salt

Giving salting examples

16

What is Encoding?

Explaining what is Encoding

17

THANK YOU

Opening the door to questions

Why Cryptography Matters

Cryptography is one of the most **important** tools **businesses** use to **secure** the **systems** that hold its most important **asset** whether it is at-rest or in-motion.

Cryptographic Algorithm

A **cryptographic** algorithm is the **mathematical** equation used to scramble the **plain text** and make it **unreadable**.

What is Plaintext?

Readable and **understandable** data that is given to an **encryption algorithm** as an **input**.

What is Ciphertext?

Output of encryption algorithm in an unintelligible form that one cannot understand.

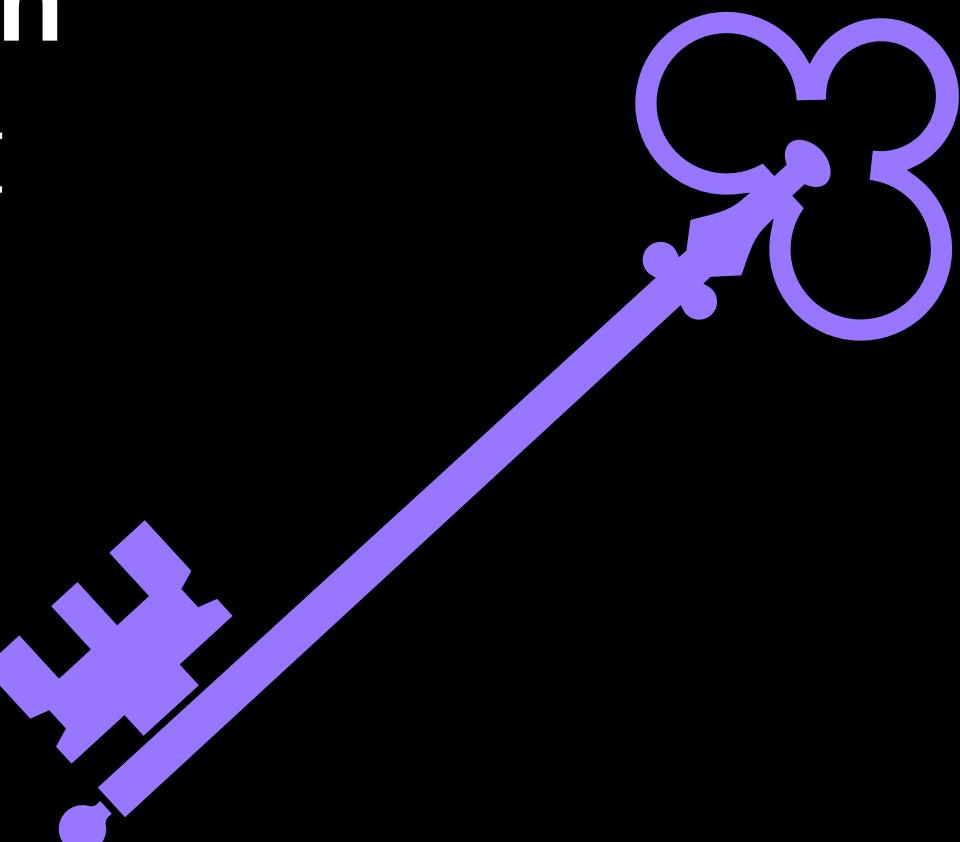


A 10x10 grid of characters, each in a different color, representing encrypted data. The characters include letters, numbers, and symbols like !, @, #, \$, %, ^, &, *, (,), :, ;, ., , etc. The colors used are blue, green, red, yellow, purple, orange, pink, brown, and black.

L	I	-	Z	P	,	W	B	M	A	-	I	#	E	Q	-	~	B	q	U	
e	/	^	~	k	i	-	%	I	r	<	#	5	N	Z	L	#	i	h	!	R
F	x	H	I	j	n	k	b	?	y	;	f	L	[+	W	1	2	0	8	T
]	N	M	,	I	y	5	W	@	^	:	u	=	<	Z	h	"	[+	_	7
I	R	p	"	b	c	\	j	D	&	r	{	%	a		#	+	2	{	W	I
Z	r	>)	*	u	S	4	g	d	J	P	a	~	1	5	d	h	{		z
3	2	P	N	W	B	~	m	t	a)	z	2	1	d	`	M	0	e	R	D
8	x	8	%	'	b		}	l	{	@	H	\$	_	u	Z	W	w	E	J	R
~	=	T	r	E	7	C	(Y	1	7	R	>	,	8	V	b	@	"	y	L
&	@	6	N	Z	!	R]	Q	w	}	b	y	u	V	[?	f	+	g	k

What is a key?

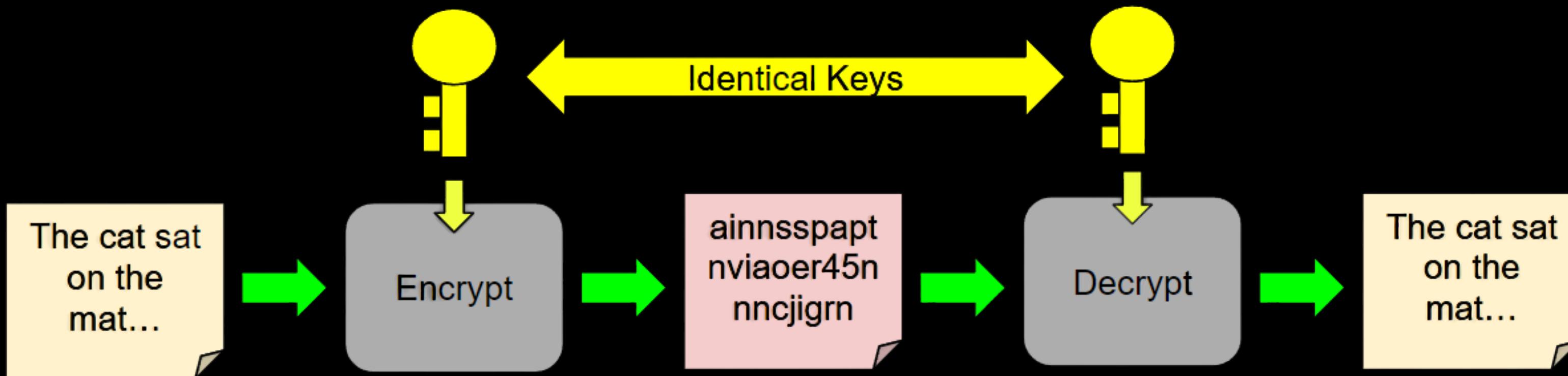
In **cryptography**, a **key** is a string of characters used within an **encryption algorithm** for **altering** data so that it **appears random**.



Symmetric Encryption

Symmetric Encryption is an **Algorithms** that use the same **cryptographic keys** for both the **encryption** of **plaintext** and the **decryption** of **ciphertext**.

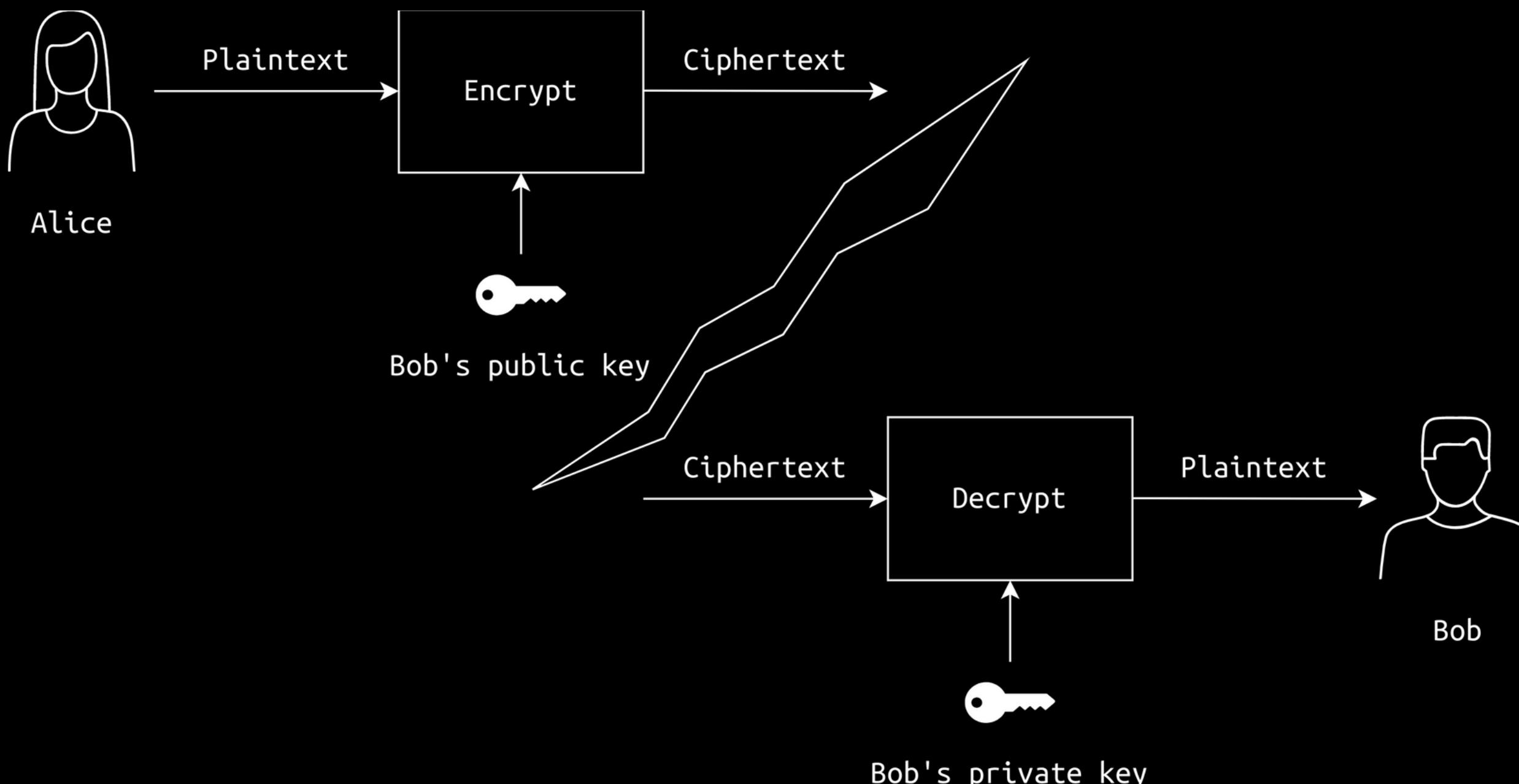
Symmetric Encryption



Asymmetric Encryption

Asymmetric Encryption or **Public-key cryptography**, uses **two different keys** - a **private key** and a **public key**. The private key is **kept secret**, while the public key is **shared freely**.

Asymmetric Encryption



RSA Algorithm

RSA is a **public-key** cryptosystem, one of the **oldest**, that is widely used for secure **data transmission**.



RSA Mathematical Representation

1. Choose two random prime numbers, p and q . Calculate $N = p \times q$.
2. Choose two integers e and d such that $e \times d = 1 \text{ mod } \phi(N)$, where: $\phi(N) = N - p - q - 1$

This step will let us generate the public key (N, e) and the private key (N, d) .

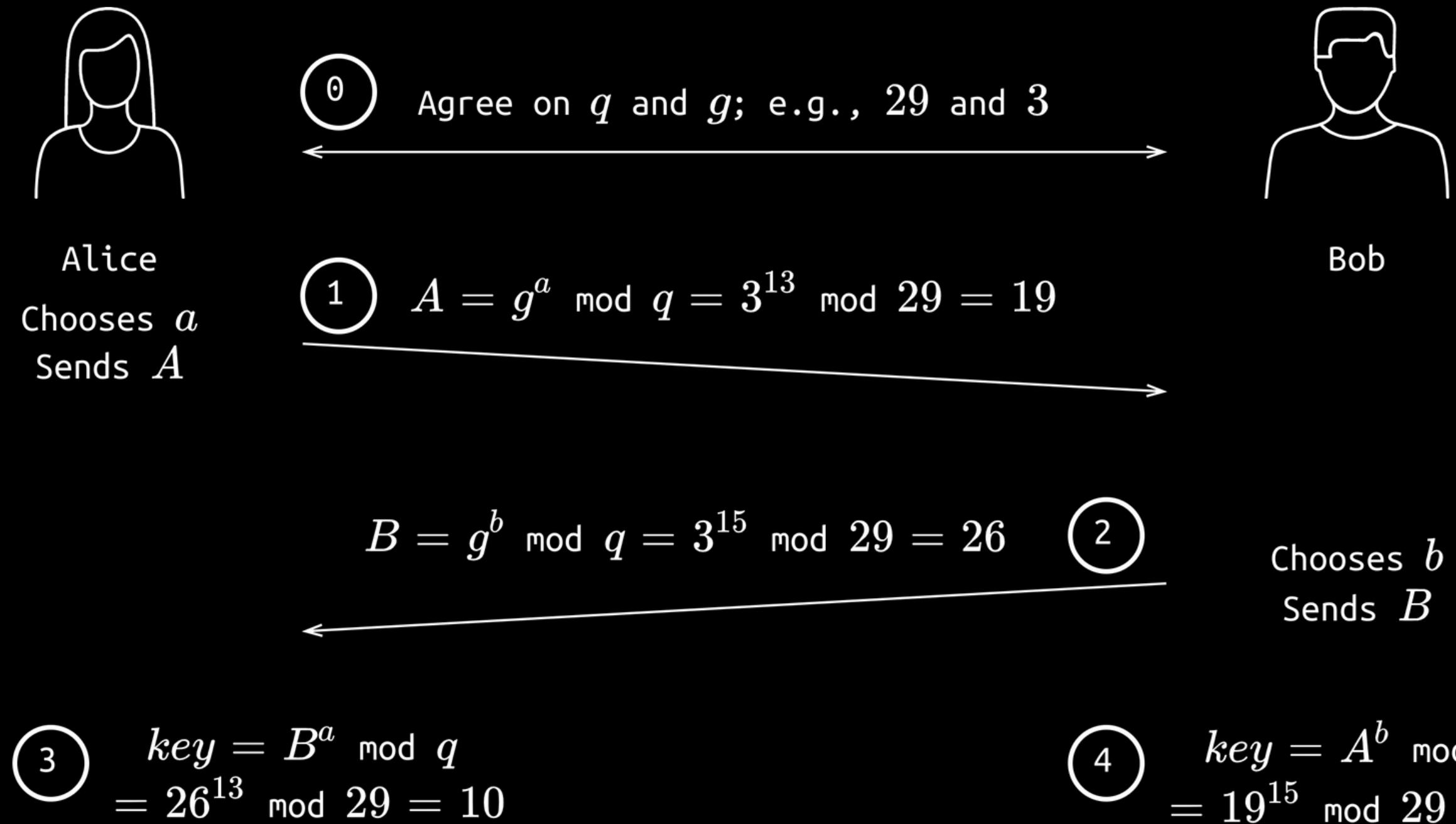
3. The sender can encrypt a value x by calculating: $y = x^e \text{ mod } N$
4. The recipient can decrypt y by calculating: $x = y^d \text{ mod } N$



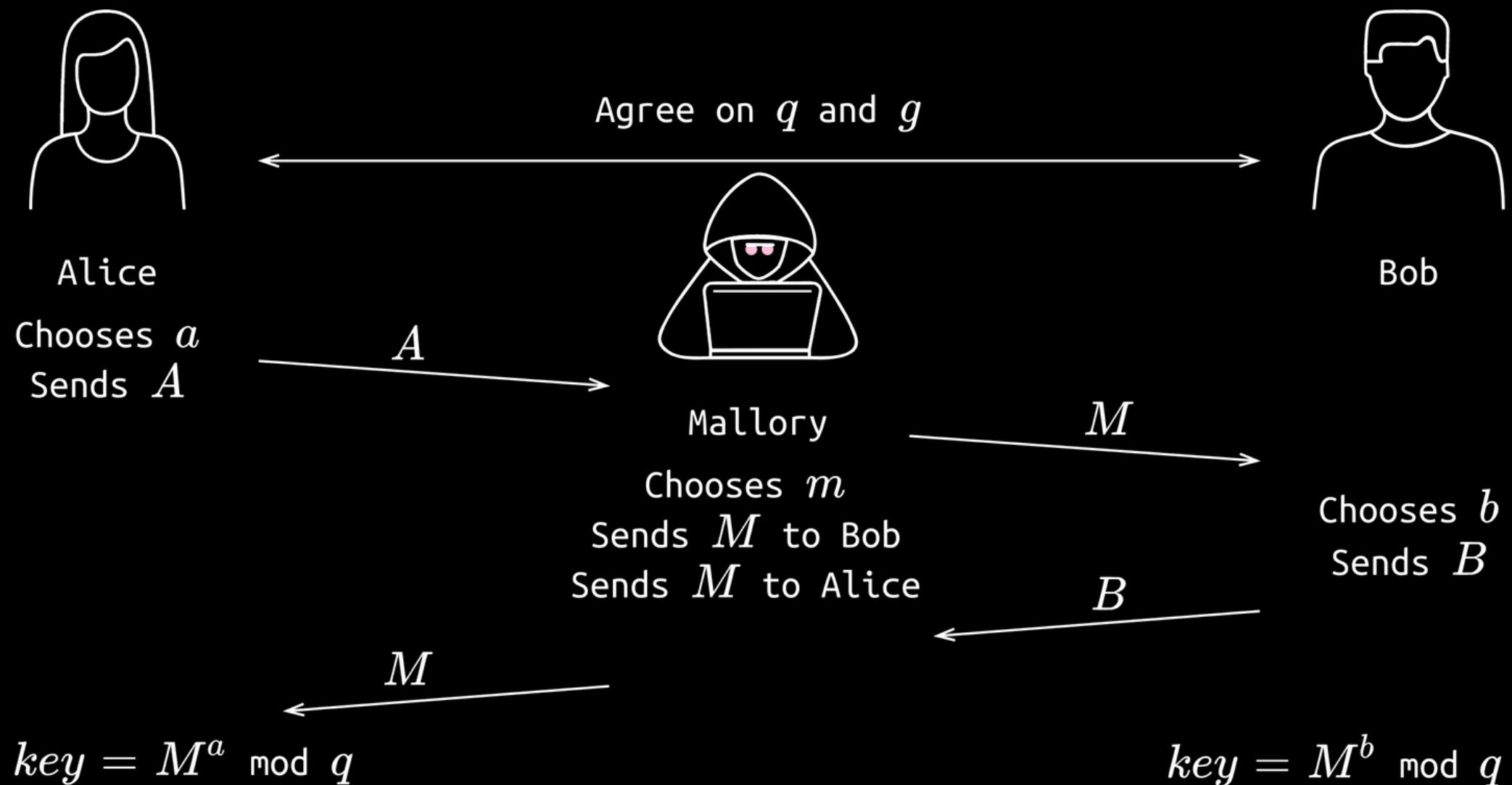
Diffie-Hellman Key Exchange

Diffie-Hellman (DH) is a cryptographic **protocol** that **enables** two parties to agree on a **shared secret key** without prior **knowledge** of each other.

Diffie-Hellman Key Exchange



Man In the Middle Attack



The Diffie-Hellman (DH) key exchange is
vulnerable to a **man-in-the-middle** attack.

Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of **rules** and **policies** that makes it possible for **different entities** to communicate **securely** over a **network**.

What is Hashing?

A **hash function** is a **mathematical algorithm** that takes an **input** (or ‘message’) and returns a **fixed-size string** of bytes, usually in the form of a **hexadecimal number**.



Message Digest Method 5

MD5 a cryptographic **hash algorithm** used to generate a **128-bit** digest from a **string of any length**.

Salting



Adding random **data** to the **input of a hash** function to **guarantee** a unique output, the **hash**, even when the **inputs are the same**.

Prepending the Salt

Password: **hello@/0-2freesh**

Salt: **datae8300kd/as**

Salted Input: **datae8300kd/ashello@/0-2freesh**

Hash (SHA-256):

f5ac26a91c388aaff9bd849a03ce888b91f1cf7474b07d68ea554d78d7426740

```
e2r1p8% echo -n "datae8300kd/ashello@/0-2freesh" | openssl sha256
SHA2-256(stdin)= f5ac26a91c388aaff9bd849a03ce888b91f1cf7474b07d68ea554d78d7426740
```

Appending the Salt

Password: hello@/0-2freesh

Salt: datae8300kd/as

Salted Input: hello@/0-2freeshdatae8300kd/as

Hash (SHA-256):

614690e6eaf823b189bae26fc046e13598d67effeee253f4231305ae1832f1e3

```
e2r1p8% echo -n "hello@/0-2freeshdatae8300kd/as" | openssl sha256
SHA2-256(stdin)= 614690e6eaf823b189bae26fc046e13598d67effeee253f4231305ae1832f1e3
```

What is Encoding?

Encoding is the process of transforming a set of Unicode characters into a **sequence of bytes**.

THANK YOU FOR YOUR ATTENTION

Any
questions?