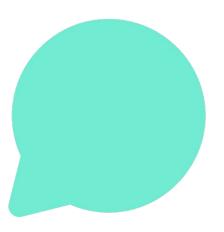
ChaChat

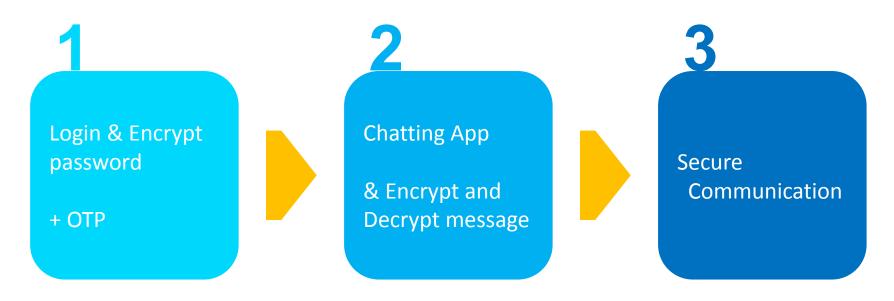
Cryptography



What is the algorithm used in this case study, and how does it work?

AIM

Chatting on Web With Cryptography Algorithms



Part 2, CODING

What is the algorithm used in this case study, and how does it work?

INFOSEC ELEMENTS

Element	Detail	Name
Confidentiality	En/Decrypt PW & Message	PBKDF2
Integrity	Hash to PW & Message	SHA256
Availability	W eb access (access anywhere)	Django
	, Backup and Sync other server	
Authenticity	Login & OTP	Django auth
Non-Repudiation	Digital Signature: HTTPS	OpenSSL

PROGRESS

What is the algorithm used in this case study, and how does it work?

FLOWCHART

HTTPS -> En/Decrypt: ChaCha20-Poly1305 **Secure Connecting** Clients Server Django http messages request Consumer View Alice (HTTP) **Function** websocket response messages Consumer Interface Channel (websocket) Server Layer Bob Background