

# PROTOKÓŁ KOMUNIKACJI + SZYFROWANIE

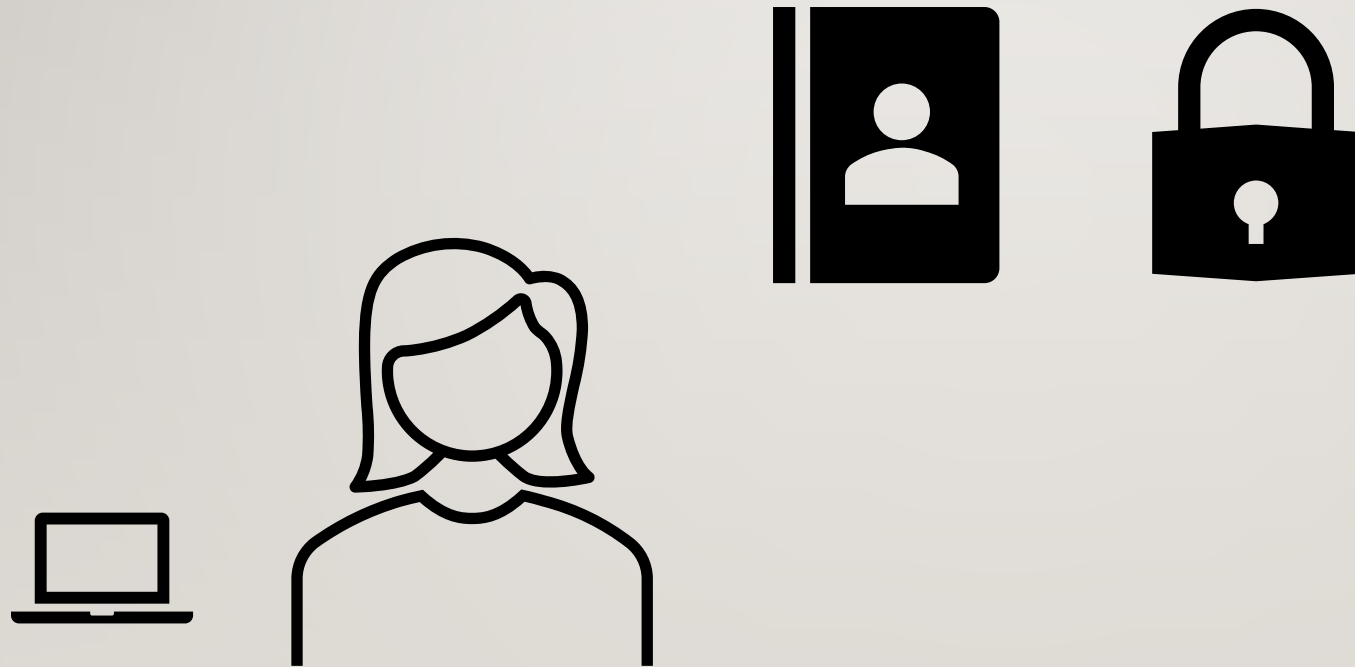
---

MAKARY GRAD | NIKODEM JAKUBOWSKI | TOMASZ LENIART | WOJCIECH  
MATUSZYŃSKI | JAKUB OLECH | ALEKSANDRA RZĄCA | SZYMON SZKARŁAT



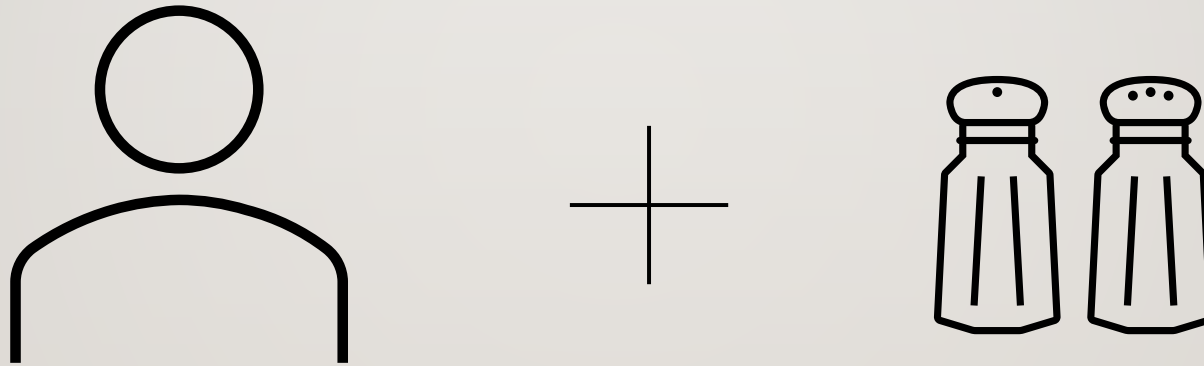
ALICJA ZAKŁADA KONTO NA KOMUNIKATORZE,  
PODAJĄC UNIKATOWY NICK I WYBIERAJĄC HASŁO

---



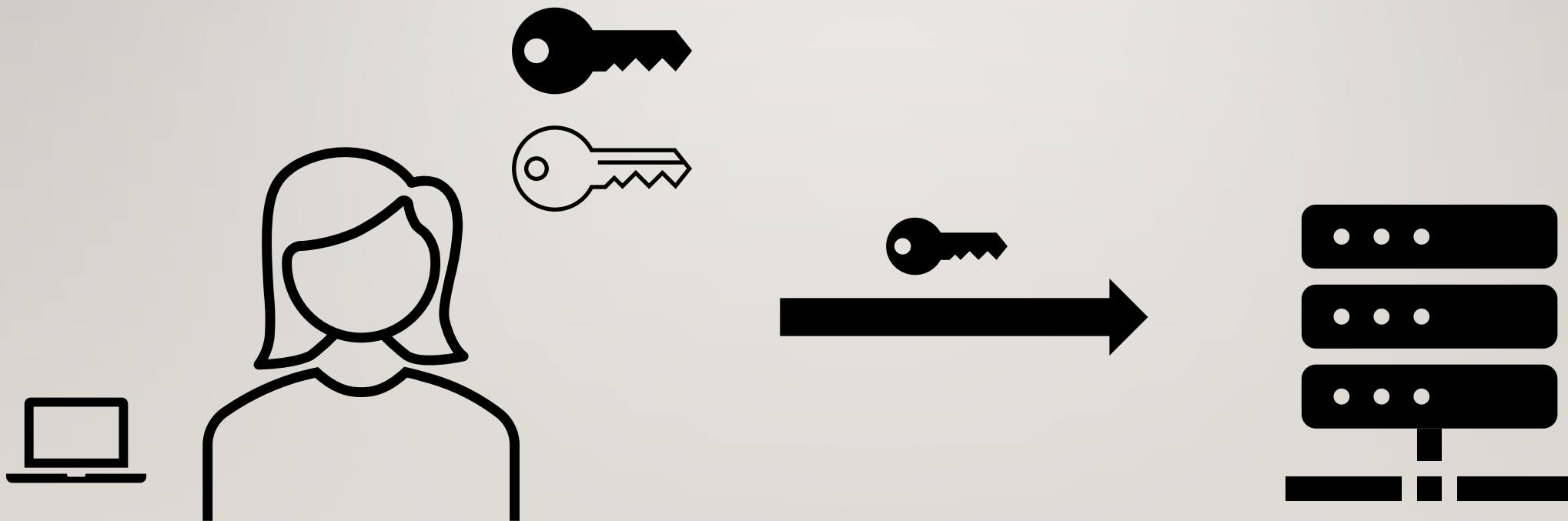
# TWORZENIE KONTA, DODANIE DANYCH UŻYTKOWNIKA DO BAZY (HASH HASŁA + SÓL)

---



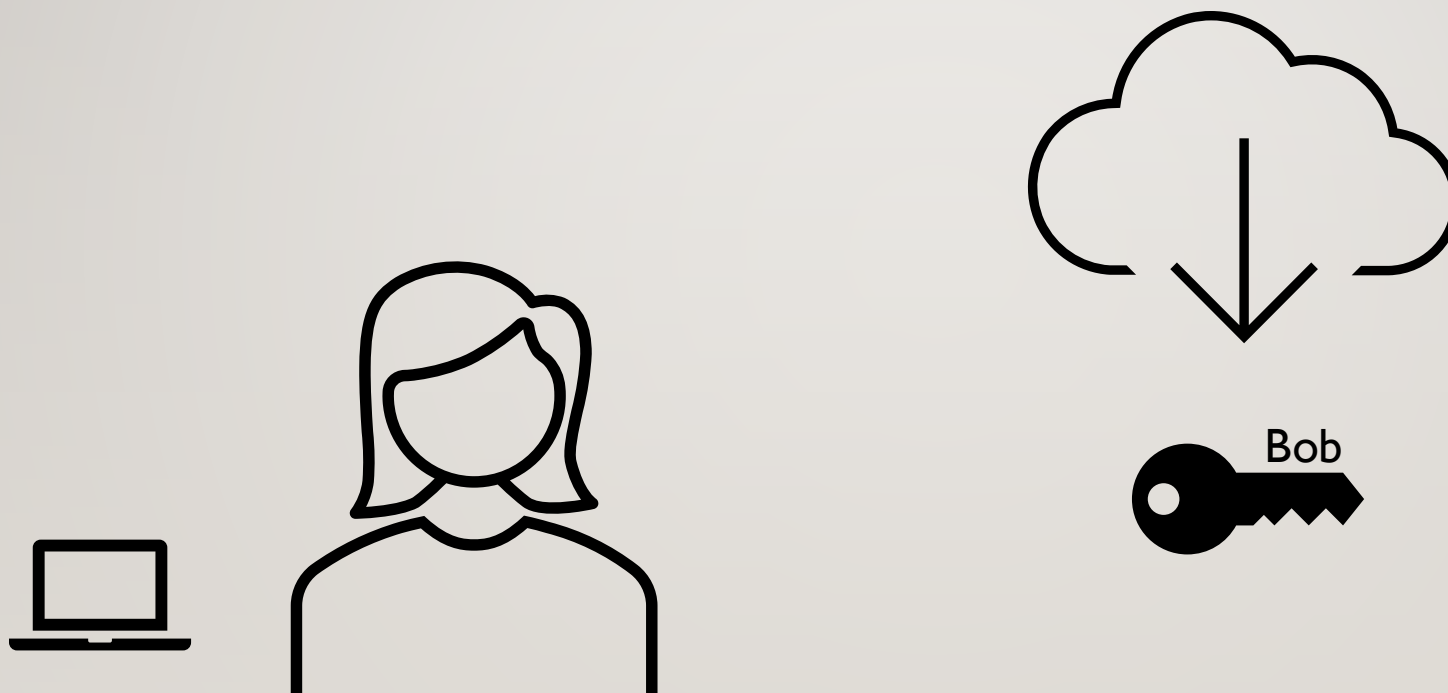
ALICJA GENERUJE PARĘ KLUCZY (PUBLICZNY,  
PRYWATNY) I WYSYŁA KLUCZ PUBLICZNY DO PKI

---



# ALICJA POBIERA Z SERWERA KLUCZ PUBLICZNY BOBA ORAZ JEGO ADRES IP

---





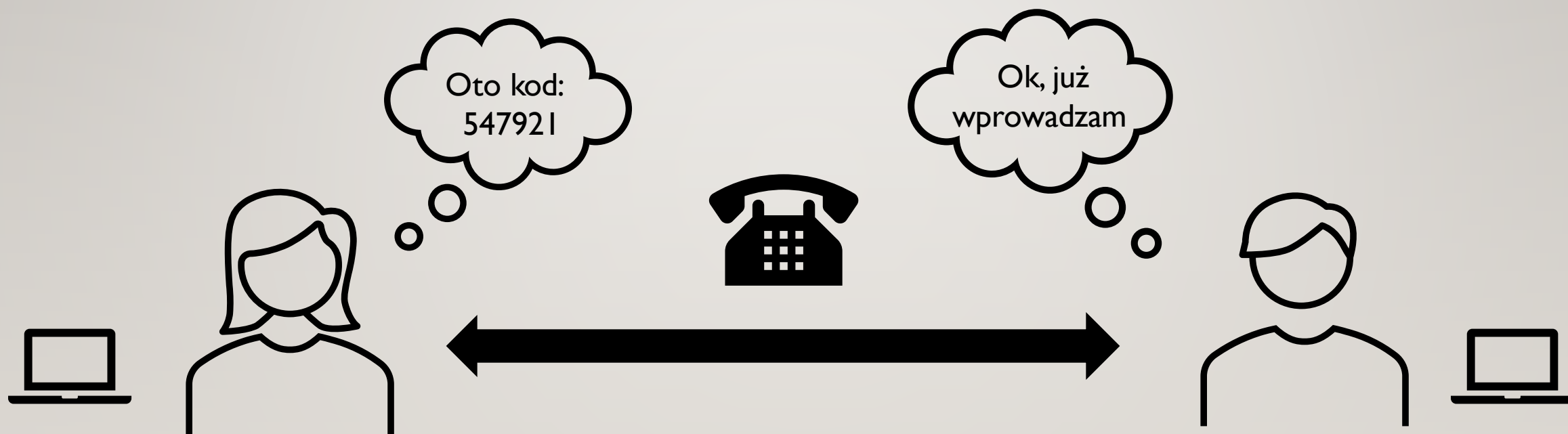
ALICJA CHCE WYŚLAĆ PLIK DO BOBA,  
BOB MUSI ZATWIERDZIĆ CHĘĆ KOMUNIKACJI

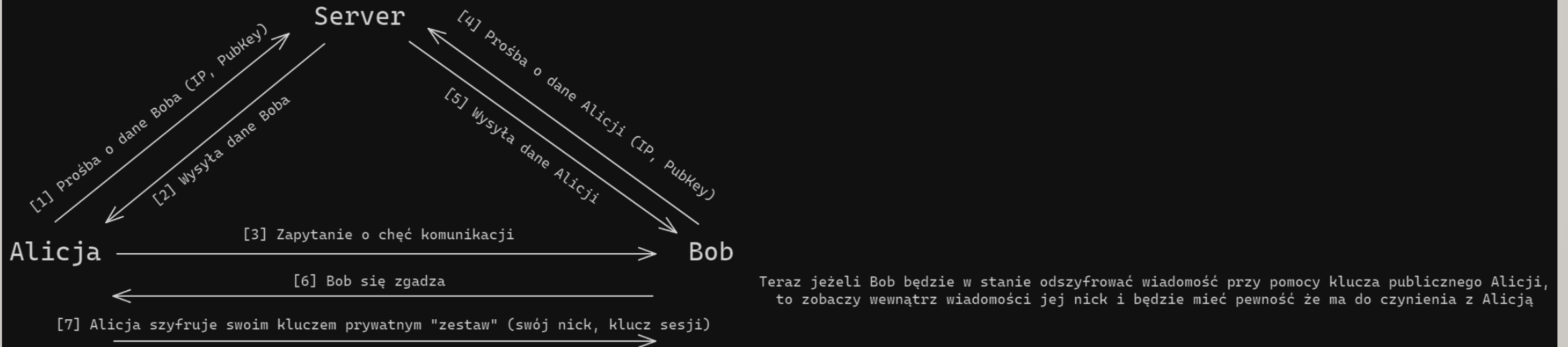
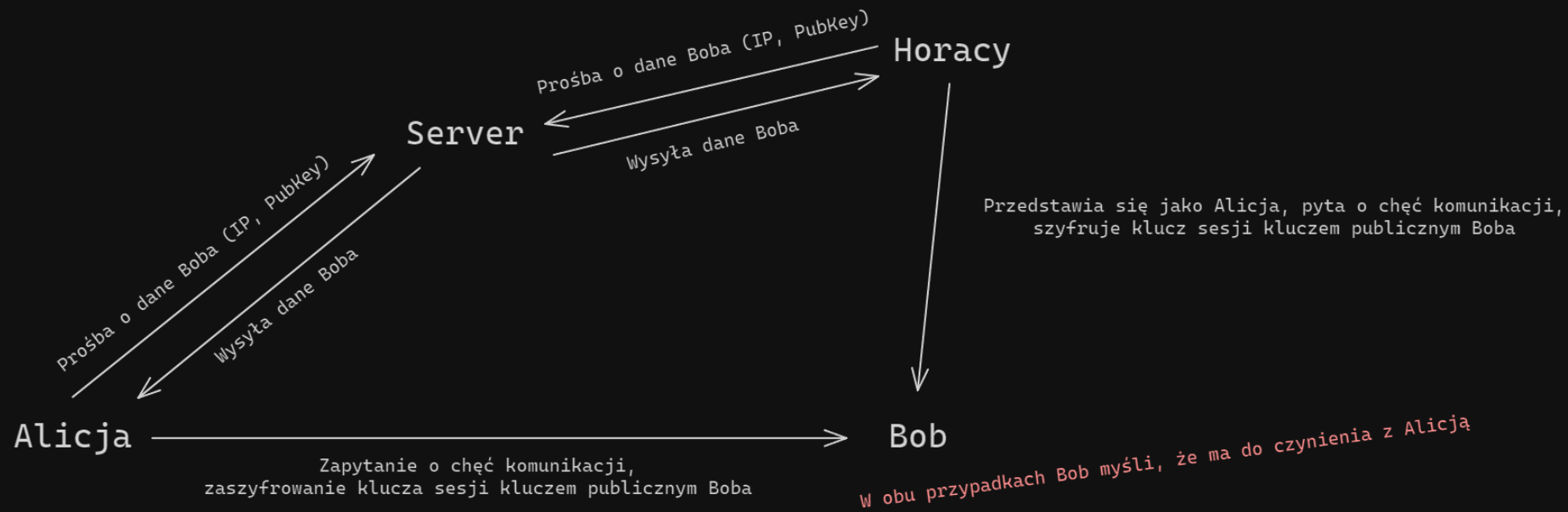
---



A TAKŻE SKONTAKTOWAĆ SIĘ Z ALICJĄ, BY  
POTWIERDZIĆ JEJ TOŻSAMOŚĆ (6-CYFROWY KOD)

---







ALICJA GENERUJE KLUCZ SESJI (SESSION-TIMEOUT),  
SZYFRUJE GO KLUCZEM PUBLICZNYM BOBA

---



ALICJA PRZESYŁA DUŻĄ ILOŚĆ DANYCH (NP.  
MULTIMEDIA) SZYFRUJĄC KLUCZEM SESJI

---



# PROTOKÓŁ KOMUNIKACJI + SZYFROWANIE

---

MAKARY GRAD | NIKODEM JAKUBOWSKI | TOMASZ LENIART | WOJCIECH  
MATUSZYŃSKI | JAKUB OLECH | ALEKSANDRA RZĄCA | SZYMON SZKARŁAT

Dziękujemy za uwagę!

