

LIFPROJET CHIFFREMENT FONDÉ SUR L'IDENTITÉ (IBE)

Groupe

Mourad ALLAM (11509098)

Nicolas EUVRARD-BLANC (11508330)

Gabriel SEQUEIRA (11508289)

Enseignant

Fabrice MOUHARTEM

SOMMAIRE

1. Le chiffrement... À quoi ça sert ?

2. Spoutnik et IBE

1. Architecture
2. Prévisualisation
3. Modules
4. Outils

3. Démonstration

4. Conclusion

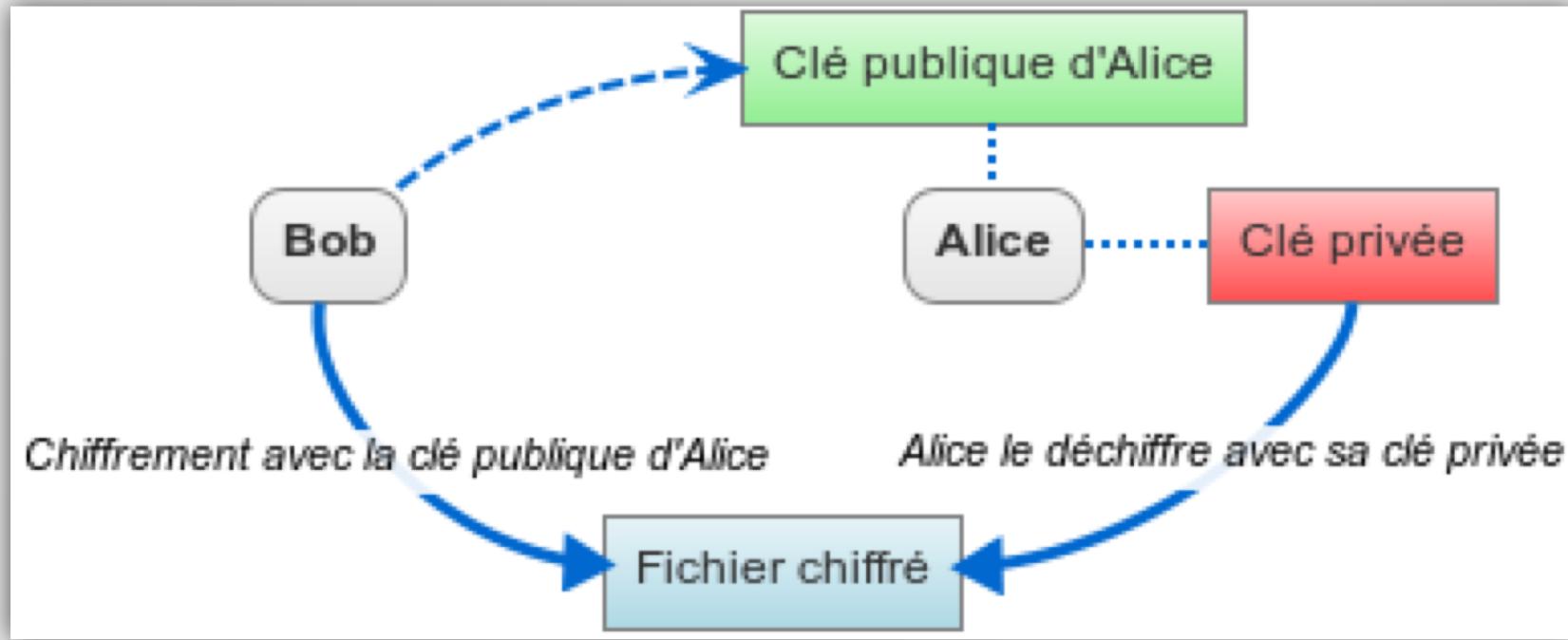
1. Difficultés rencontrées
2. Améliorations
3. Ce que ça nous a apporté

1 - CHIFFREMENT... À QUOI ÇA SERT ?

- Transmettre
- Inintelligible
- Secret



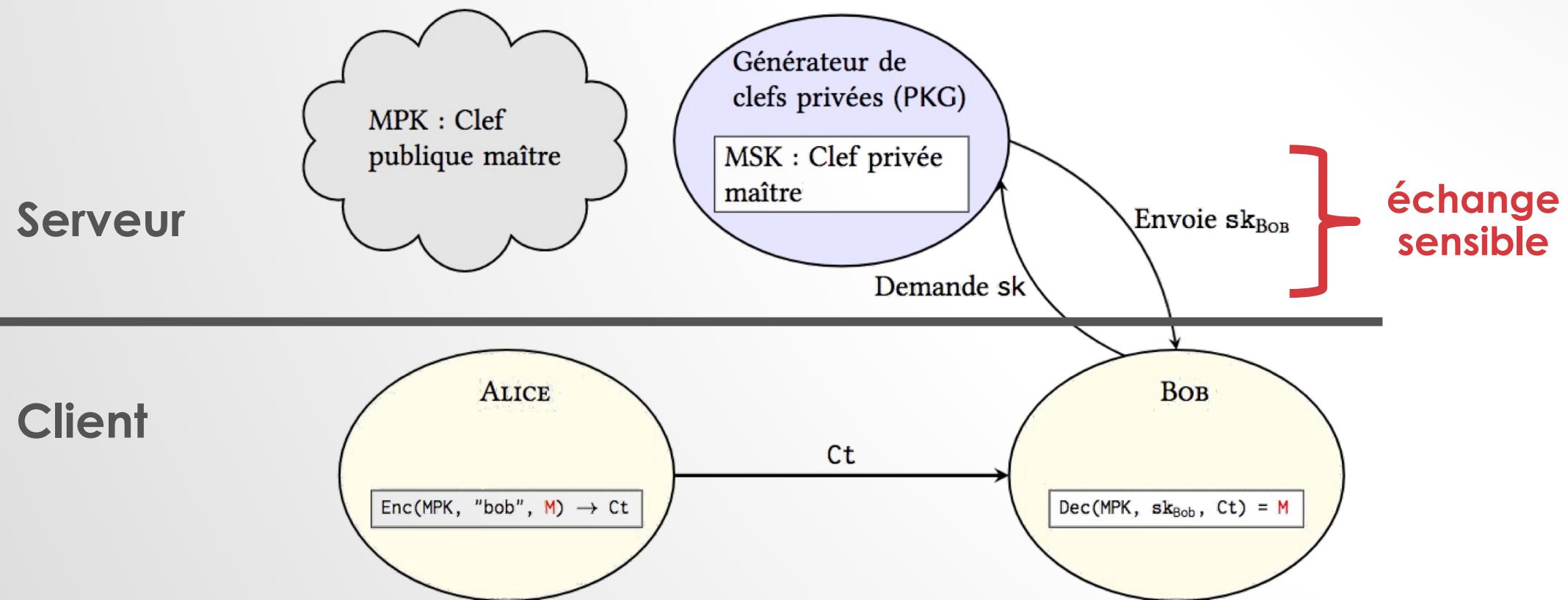
1 - CHIFFREMENT... À QUOI ÇA SERT ?



Notre proposition : IBE de Cocks et AES

2 - SPOUTNIK ET IBE

1. Architecture
 - Client / Serveur



2 - SPUTNIK ET IBE

2. Chronologie (Gantt)

| | 29/01 | 30/01 | 05/02 | 06/02 | 12/02 | 13/02 | 26/02 | 27/02 | 05/03 | 06/03 | 12/03 | 13/03 | 19/03 | 20/03 | 26/03 | 27/03 | 03/04 | 09/04 | 10/04 |
|--------------------------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| Recherches (RSA, AES, GMP, IBE, ...) | | | | | | | | | | | | | | | | | | | |
| Début avec la librairie GMP | | | | | | | | | | | | | | | | | | | |
| Répartition des tâches à effectuer | | | | | | | | | | | | | | | | | | | |
| Module Chiffrement | | | | | | | | | | | | | | | | | | | |
| Module PKG | | | | | | | | | | | | | | | | | | | |
| Module Socket | | | | | | | | | | | | | | | | | | | |
| Module Dechiffrement | | | | | | | | | | | | | | | | | | | |
| Module Outils | | | | | | | | | | | | | | | | | | | |
| Module Mail | | | | | | | | | | | | | | | | | | | |
| Intégration de Qt | | | | | | | | | | | | | | | | | | | |
| Documentation du code (doxygen) | | | | | | | | | | | | | | | | | | | |
| Intégration d'IMAP | | | | | | | | | | | | | | | | | | | |
| Nettoyage avant le rendu | | | | | | | | | | | | | | | | | | | |

2 - SPOUTNIK ET IBE

3. Outils



OpenSSL



3 - DÉMONSTRATION

Compilation TXT + Qt

Lancer le serveur

Lancer le client (fenêtre fonctionne)

Montrer que SMTP fonctionne

Montrer que le déchiffrement fonctionne

4 - CONCLUSION

1. Difficultés rencontrées

- début avec GMP
- documentation pas toujours de qualité
- hash de l'ID
- enregistrer le cipher dans un fichier texte puis le lire
- utiliser IMAP !!
- IP bloquées (spam)

4 - CONCLUSION

2. Améliorations

- Multidestinataires des mails
- pièces jointes
- IMAP (prochainement)

4 - CONCLUSION

3. Ce que ça nous a apporté

Découverte de IBE

Découverte de bibliothèques (GMP, openSSL, Curl)

Travail en groupe

Développement d'interface graphique