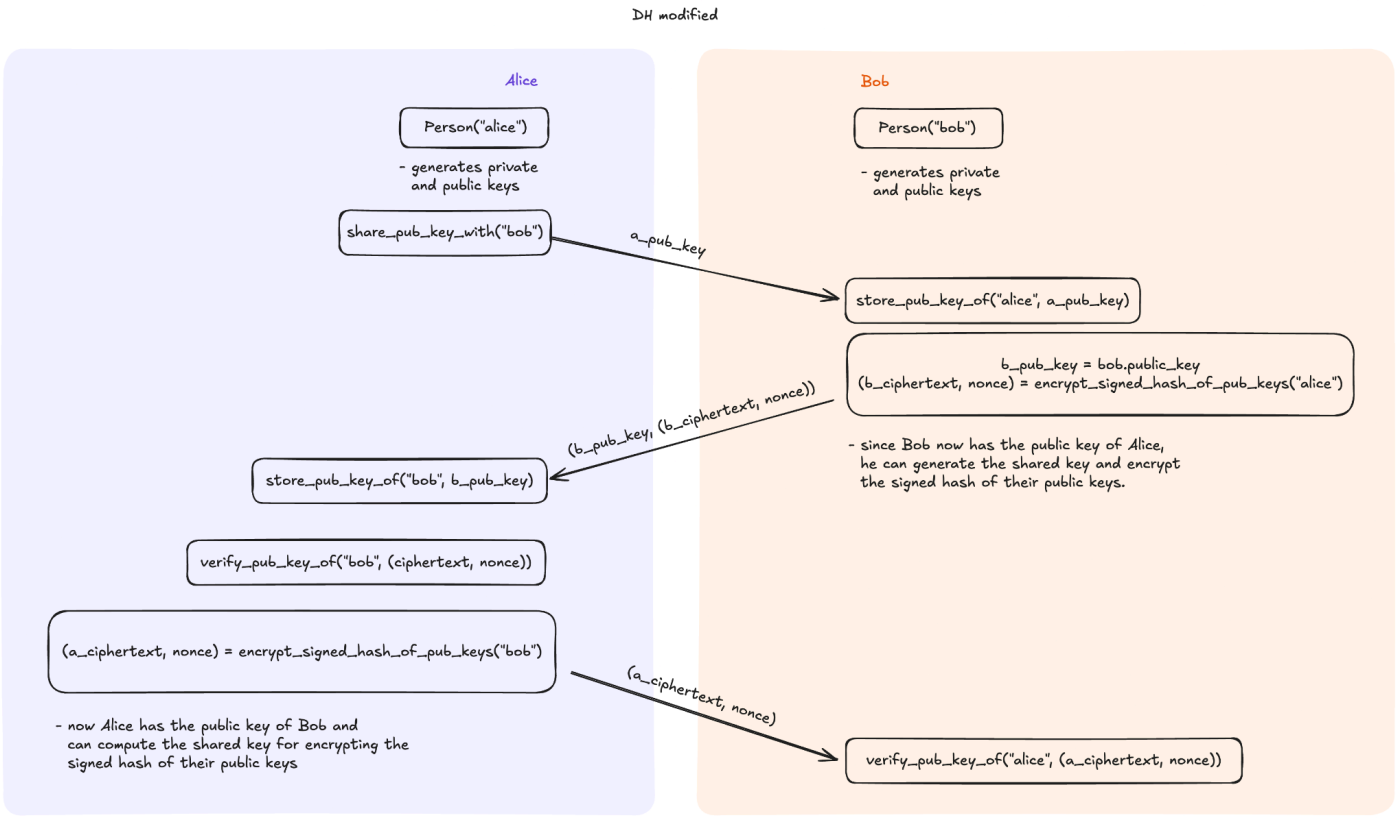
Модифицирана верзија на DH протоколот за размена на клучеви

Милена Кукољ 186085



Во првиот чекор се иницијализираат два објекти од класата Person. При самата иницијализација се генерираат приватниот и јавниот клуч за тој човек.

Овој модифициран алгоритам за размена на клучеви користи имплементација на DH со елиптични криви ECDH и имплементација на DSA со елиптични криви ECDSA. Оваа измена е потребна доколку сакаме да може приватниот и јавниот клуч да бидат компатибилни, за да се искористат истите клучеви и во двата алгоритми.

Во примерот на сликата, Алис прва го испраќа својот јавен клуч на Боб. Тој го зачувува клучот на Алис во мапа од имиња на познаници. Како клуч во оваа мапа е името на познаникот, а вредноста е торка од јавниот клуч на познаникот, нивниот заеднички клуч, и дали е верифициран тој клуч. Сега за сега Боб го зачувува јавниот клуч на Алис и нивниот заеднички клуч.

Следниот чекор е на Боб. Тој сака да го испрати својот јавен клуч на Алис. Но сака и со заедничкиот клуч да енкриптира пораката за Алис. Се користи AES алгоритамот за енкрипција затоа што користи симетрични клучеви за енкрипција и декрипција. Пораката која што сака Боб да ја прати е потпишана хаширана вредност од нивните јавни клучеви.

За да се може да се потпише пораката со приватниот клуч користејќи го ECDES алгоритамот треба да бидат јавните клучеви серијализирани во бајти.

Заштита против нападот man-in-the-middle

На овој начин не се попречува man-in-the-middle нападот. Во овој пример Вики ќе го наречеме човекот што прислушкува разговор помеѓу Алис и Боб.

1. Алис го праќа на Боб својот јавен клуч.
2. Вики го попречува праќањето и наместо на Алис јавниот клуч, го праќа својот на Боб.
3. Боб го добива лажниот јавниот клуч на Алис и генерира таен споделен клуч со јавниот клуч на Вики.
    a. Ја енкриптира својата потпишана хаширана вредност од нивните јавни клучеви
    b. Го испраќа својот јавен клуч, заедно со енкриптираната порака, на Алис
4. Вики повторно ја попречува и оваа порака.
    a. Може да ја декриптира пораката од Боб, но не може да направи ништо на потписот. Затоа генерира нов лажен потпис со заедничкиот клуч на Вики и Алис и ја енкриптира потпишаната хаширана вредност на нивните јавни клучеви.
5. Вики е сега целосно вклучена во разговорот помеѓу Алис и Боб.

За успешно да се попречи man-in-the-middle нападот потребно е да постои некој автентикациски сервер кој што ќе ги автентицира клучевите. Истотака доколку претходно бил некако потврден јавниот клуч на една од страните, овој напад не би бил возможен.