Intercambio de claves de Diffie–Hellman

Clase 14

https://apuntes.indcpa.com
Versión 0.0.1, junio 2024

- Hasta 1970, toda la criptografia utilizada era de clave simetrica.
- Esto no era una grande limitación dado que el uso principal era militar, donde "canales seguros" de intercambio de clave fisicos existen.
- Esta es una gran limitacion para uso civil.
- Vamos ahora a introducir brevemente el intercambio de claves (KEX, "key exchange") de Diffie y Hellman.
- Lo hacemos por motivos informaciónales e históricos, al ser el primer protocolo de PKC considerado seguro.
- No vamos a intentar demostrar su seguridad en detalle, porque los modelos de seguridad de KEX pueden ser muy complicados.

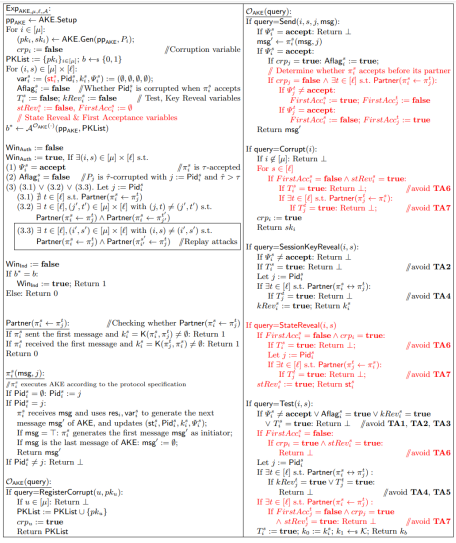
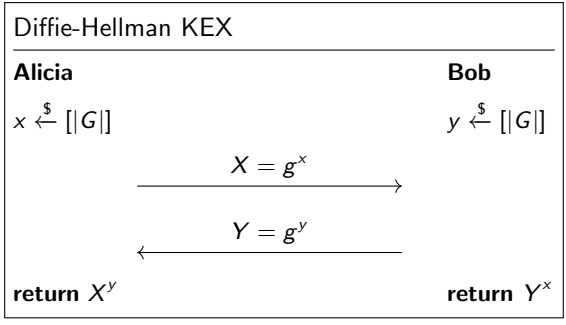


Fig. 5. The security experiments $\mathsf{Exp}^{b}_{\mathsf{AKE},\mu,\ell,\mathcal{A}}$: $\boxed{\mathsf{Exp}^{\mathsf{replay}}_{\mathsf{AKE},\mu,\ell,\mathcal{A}}}$ (both without red text) and $\boxed{\mathsf{Exp}^{\mathsf{replay,\ state}}_{\mathsf{AKE},\mu,\ell,\mathcal{A}}}$ (with red text). The list of trivial attacks is given in Table 2.

Modelo de seguridad de intercambio de clave autenticado usado en Han *et al.*, CRYPTO 2021.

Supongamos que dos partes Alicia y Bob se ponen de acuerdo publicamente sobre un grupo cíclico finito $\mathbb{G}$ y sobre un generador g, tal que $\mathbb{G} = \langle g \rangle$.



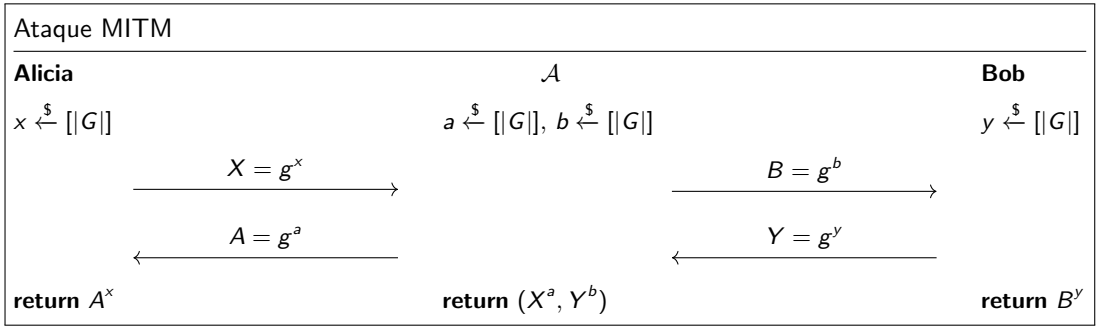
- Notamos que $X^y = (g^x)^y = g^{xy} = g^{yx} = (g^y)^x = Y^x$.
  - Alicia y Bob retornan el mismo elemento $g^{xy} \in \mathbb{G}$.
- Podemos definir una función de hash $H \colon \mathbb{G} \to \{0,1\}^\ell$, y utilizar $H(g^{xy})$ como clave para cifrado (simetrico) autenticado.
  - Formalmente, se precisa que H sea una función de derivacíon de claves (KDF, key-derivation function).

Definir la seguridad del KEX puede ser complicado. Supongamos un adversario que se limita a observar pasivamente la comunicacion (el "transcript") (g^x, g^y).

- Si CDH es difícil en $\mathbb{G}$, sabemos que calcular g^{xy} es difícil.
- Es esto sucficiente a garantizar que DH es seguro frente a un adversario "pasivo" (que solo observa trafico de red)? CDH no excluye que "mitad de los bits" de g^{xy} sean aprendibles. Esto podria teoricamente resultar en vulnerar la siguiente fase de comunicacion.
  - Junto a un hash, esto es suficiente en el Random Oracle Model, *c.f.* § 11.5.1 **BS**.
- De aqui la idea de usar DDH: si (g^x, g^y, g^{xy}) es indistinguible de (g^x, g^y, g^z) con z aleatorio, $\mathcal{A}$ aprende "nada" sobre xy observando (g^x, g^y).

- Notamos también que $\mathcal{A}$ podria no limitarse simplemente a observar trafico, y también interceptarlo si tiene control sobre la red.
- Este tipo de ataque se llama machine-in-the-middle (MITM).

Ataque MITM



- En este caso $\mathcal{A}$ podria fingir de ser Bob a Alice, y Alicia a Bob.
- Por ejemplo, podria interceptar $\mathrm{Enc}(H(g^{ax}), m)$ de Alicia a Bob, decifrarlo, volverlo a cifrar como $\mathrm{Enc}(H(g^{by}), m)$, y finalmente mandarlo a Bob. Alicia y Bob no podrian detectar el ataque.

- Este tipo de tactica no funcióna si Alice y Bob intercambian claves secretas de persona, y utilizan exclusivamente criptografia simetrica.
- En el setting de criptografia de clave publica, defendernos de este tipo de tactica requiere nuevos instrumentos, para construir una "infraestructura de claves publicas" (PKI, public-key infrastructure).
  - En lugar de iniciar intercambio de claves en el momento, usaremos esquemas de cifrado de clave publica (PKE, "public-key encryption"), donde Bob primero publica una clave pk, y Alicia cifra usando pk.
  - La clave de Bob va a ser "certificada" como autentica usando un sistema de firma digital.
  - Con estas tecnicas, podremos verificar la identidad de un posesor de clave publica, evitando que $\mathcal{A}$ nos engañe en cifrar hacia una clave que no le pertenece a Bob.

Empezamos entonces definiendo y construyendo PKE.