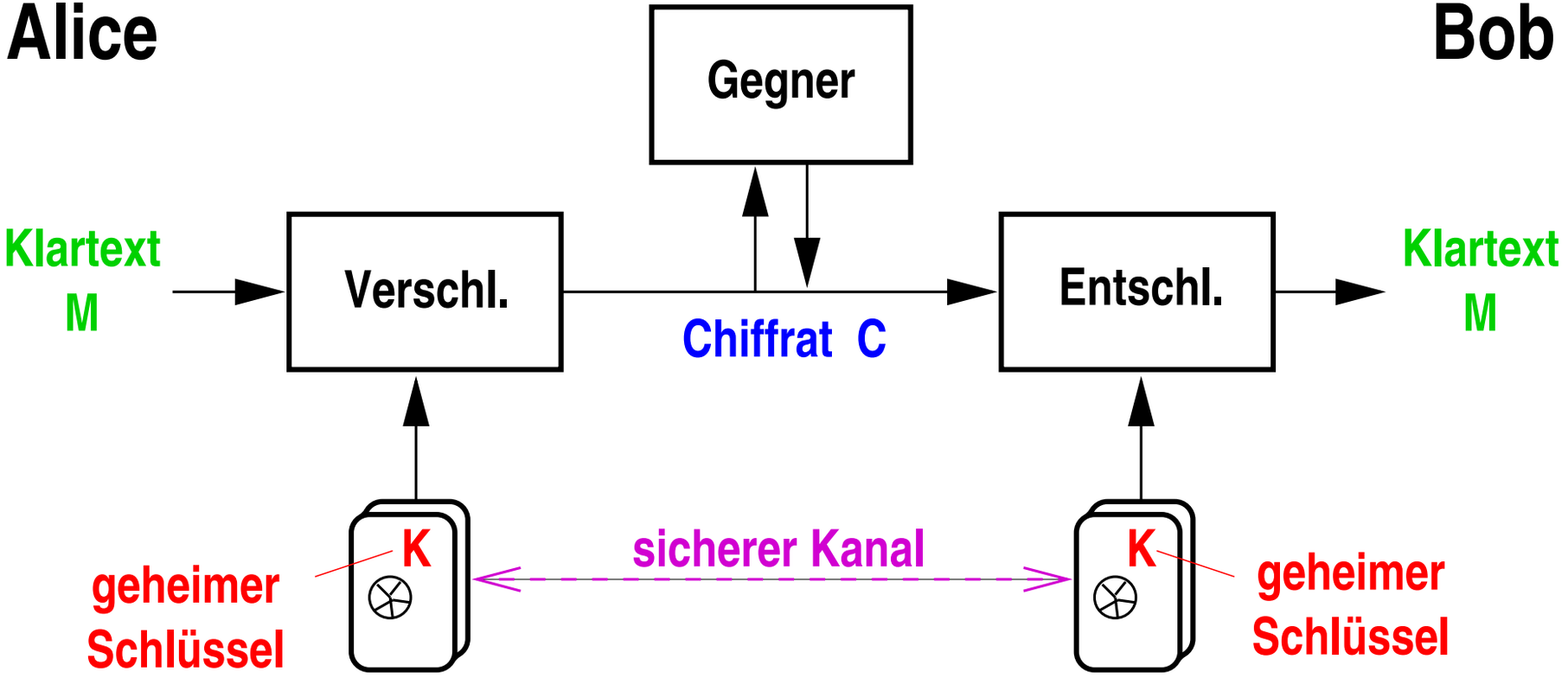
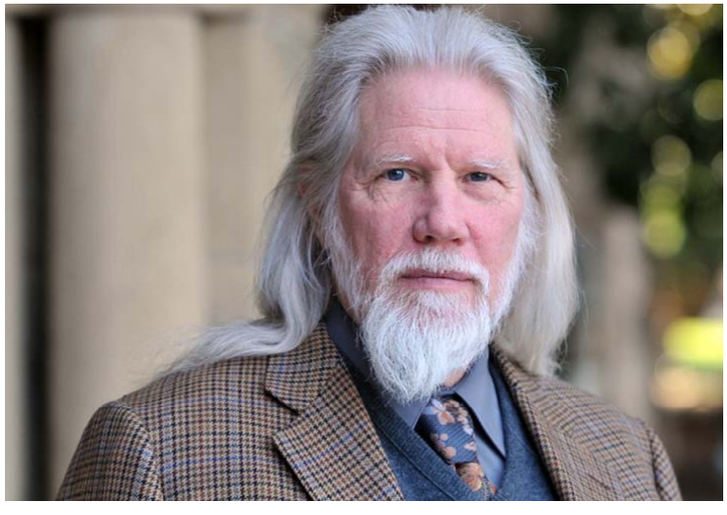
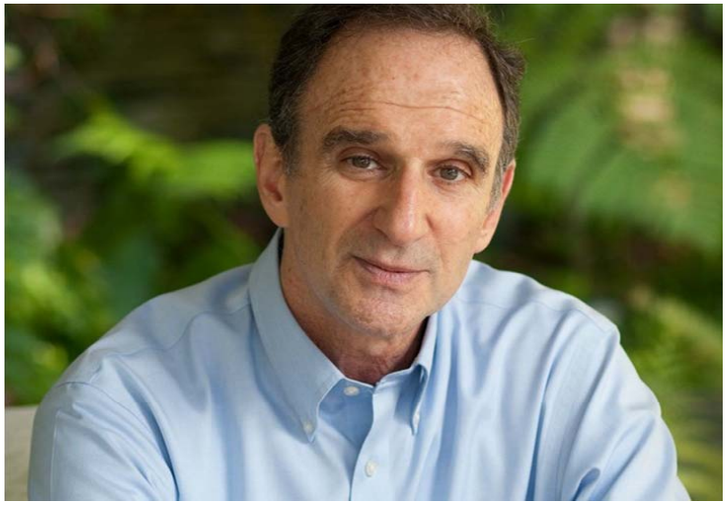
Verschlüsselungssystem





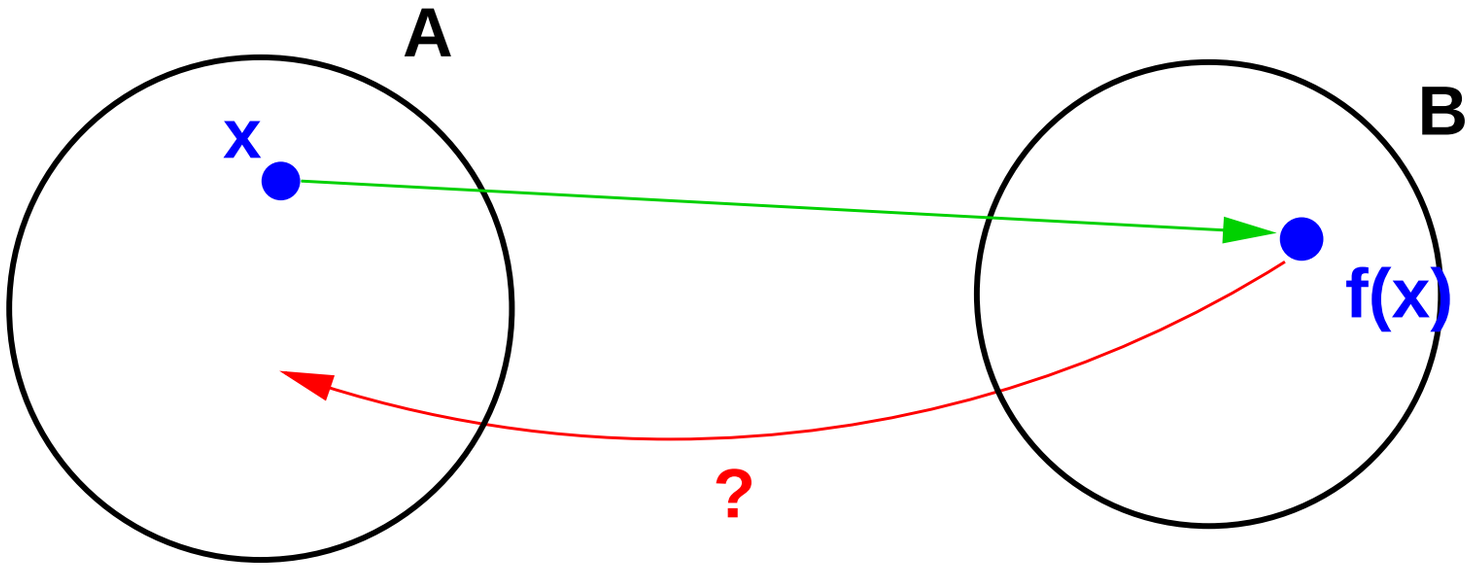
Whitfield Diffie (*1944)



Martin Hellman (*1945)

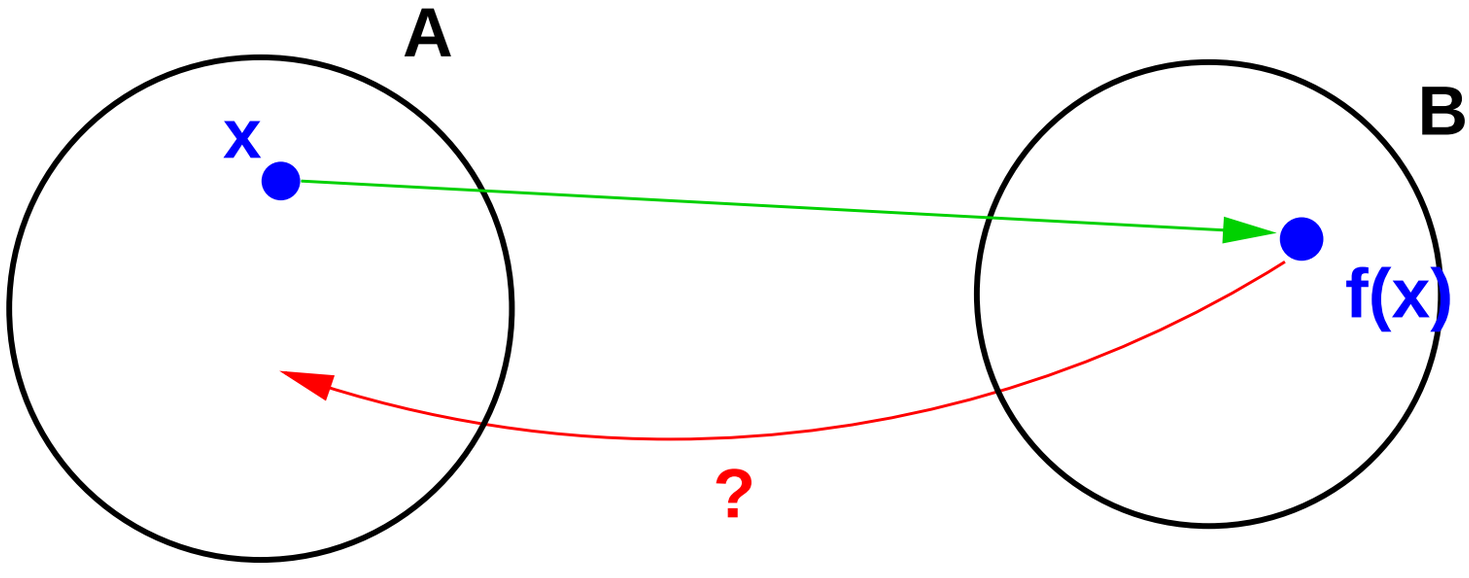
Erfinder der Public-key Kryptographie

Einwegfunktion f



f(x) ist einfach berechenbar für jedes x.

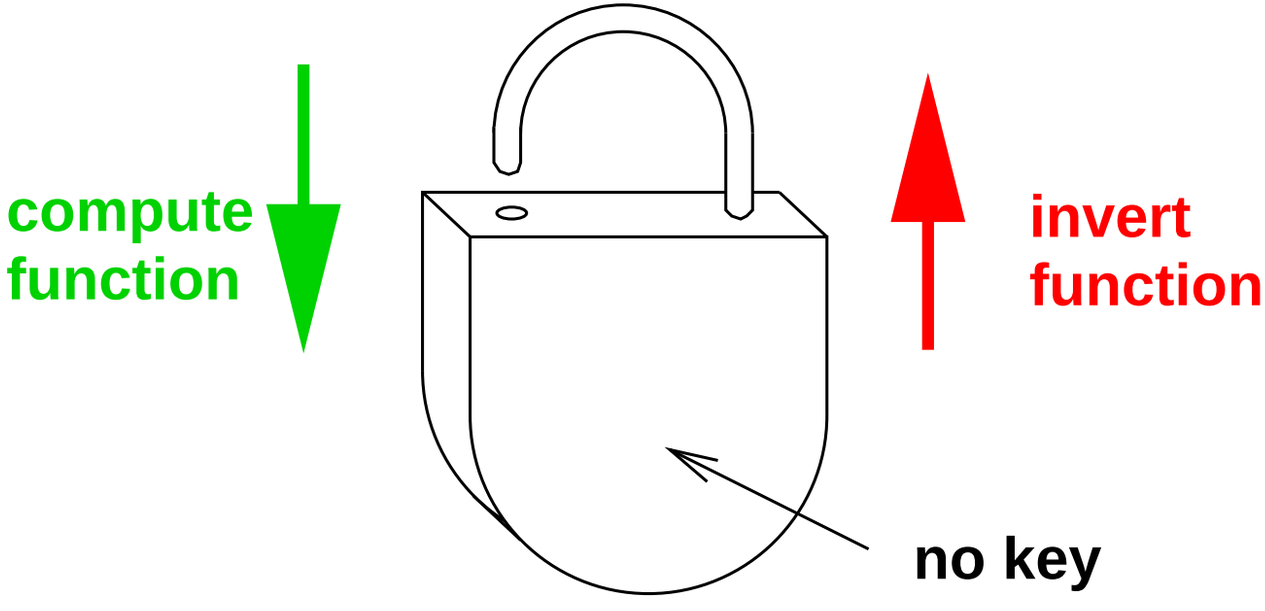
Einwegfunktion f



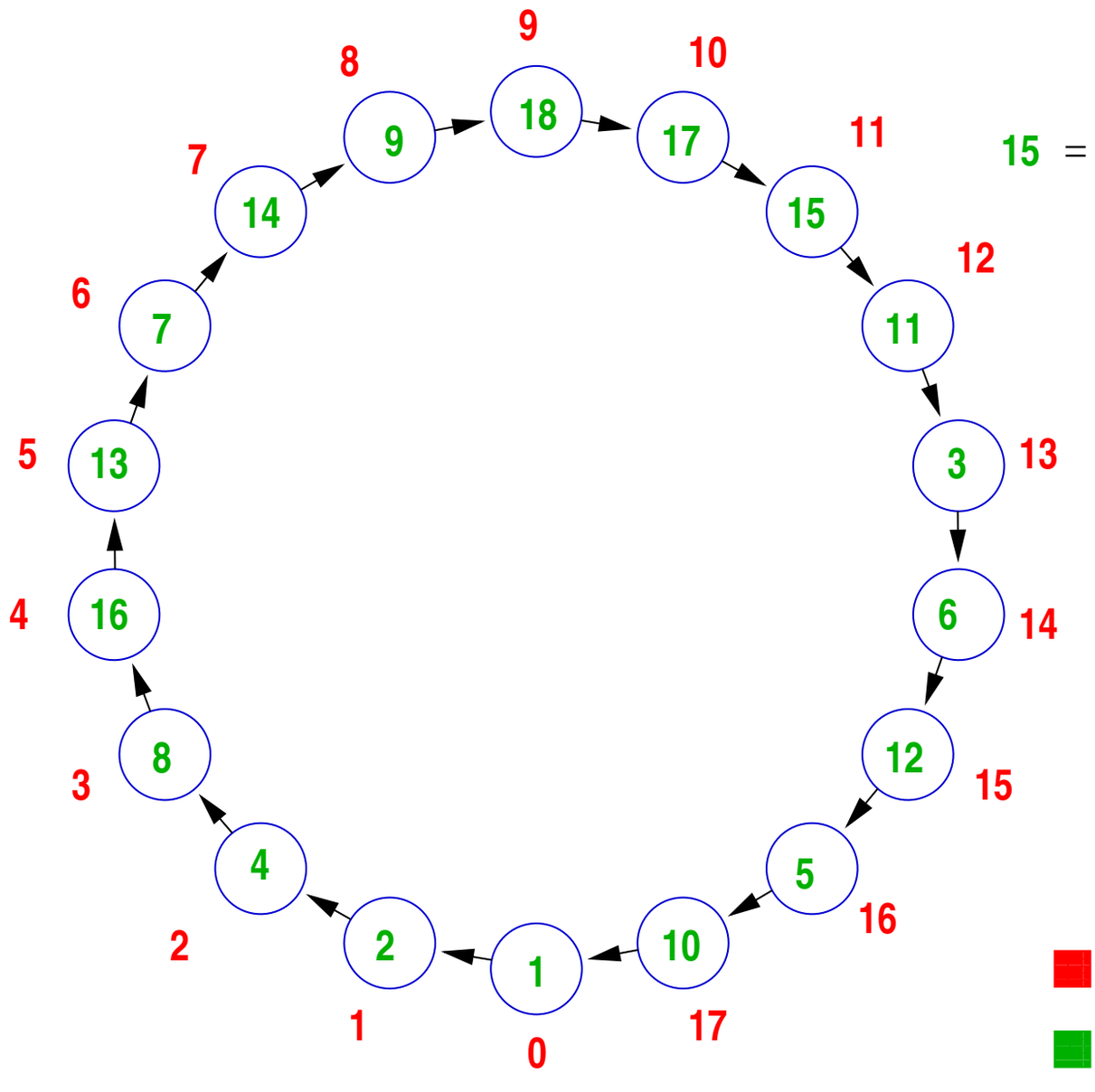
f(x) ist einfach berechenbar für jedes x.

Für zufälliges y ist es berechenmässig zu schwierig, ein x mit f(x) = y zu finden.

Einwegfunktion: Mechanisches Analogon



Potenzierung modulo 19



$15 = 2^{11} \pmod{19}$

discrete logarithm

element of group

Diffie-Hellman protocol

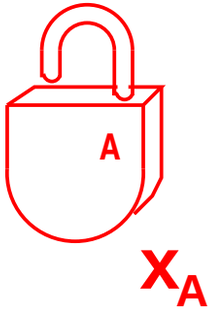
Alice **Bob**

insecure channel

Diffie-Hellman protocol

Alice **Bob**

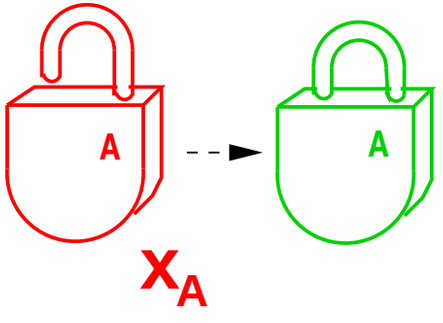
insecure channel



Diffie-Hellman protocol

Alice **Bob**

insecure channel



x_A

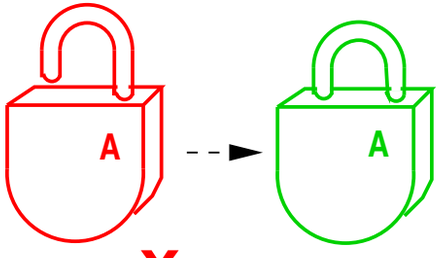
$y_A = g^{x_A}$

Diffie-Hellman protocol

Alice

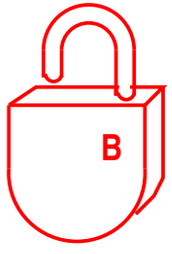
Bob

insecure channel



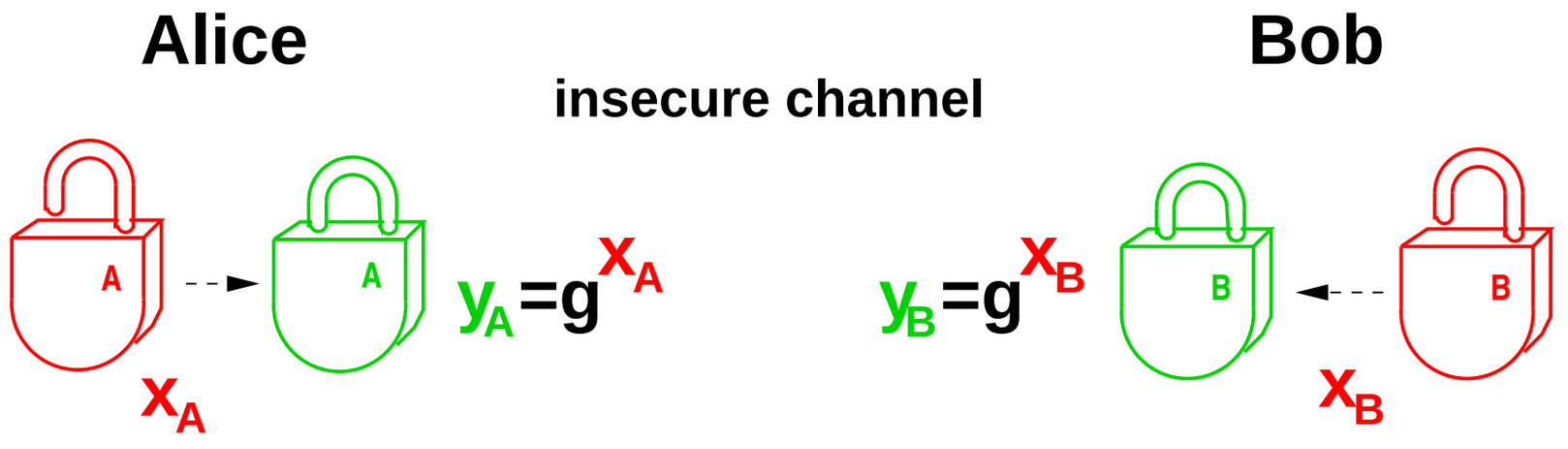
x_A

$y_A = g^{x_A}$

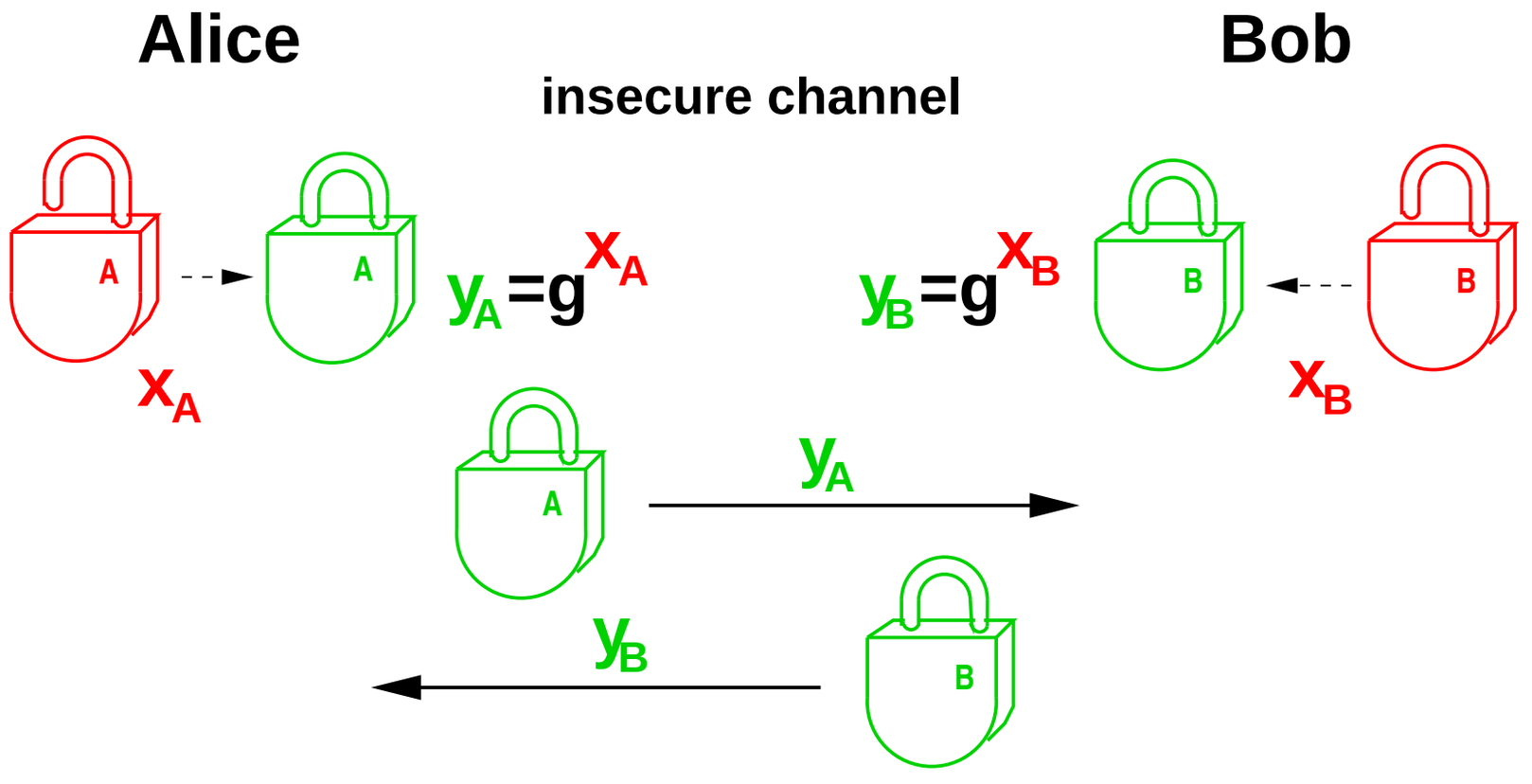


x_B

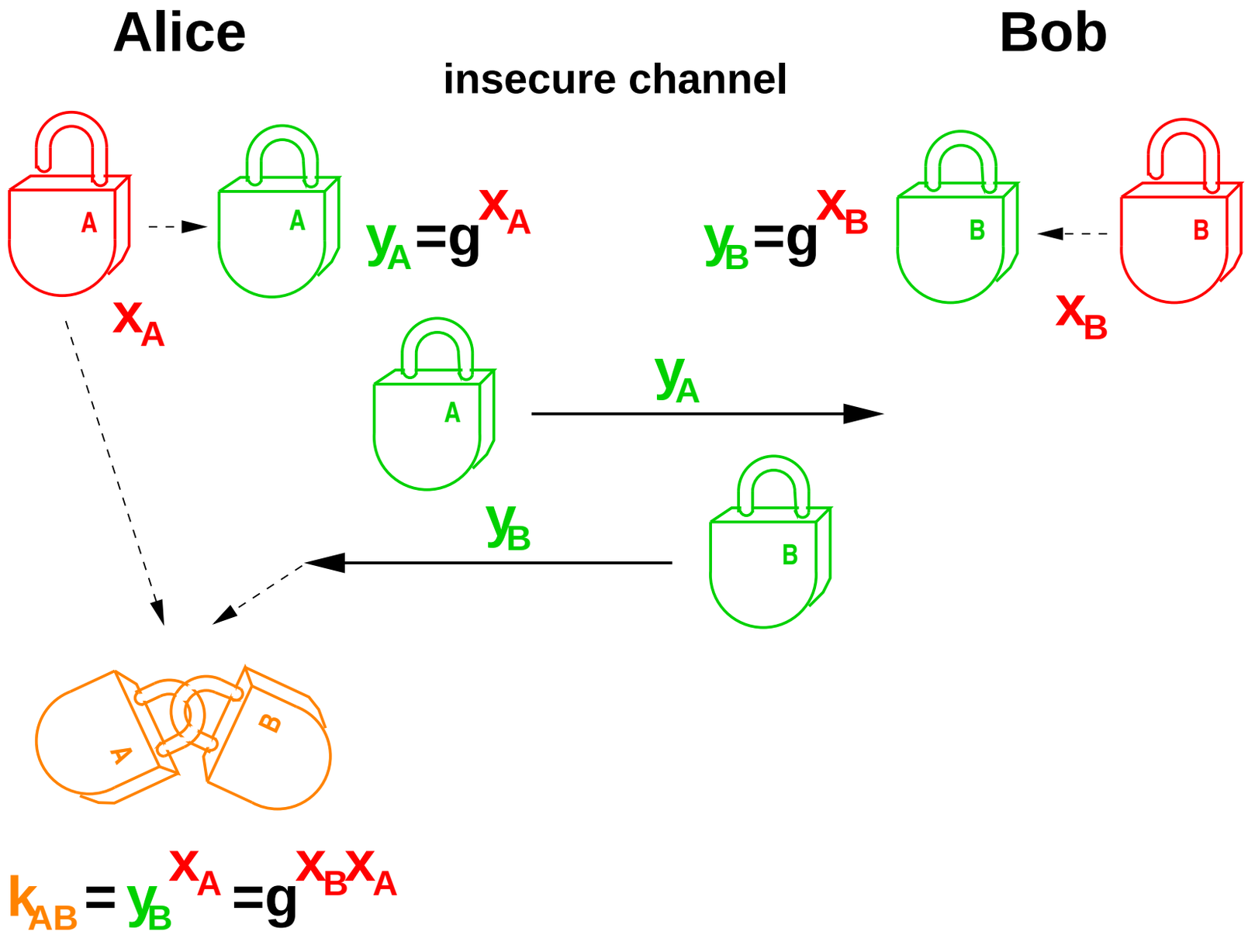
Diffie-Hellman protocol



Diffie-Hellman protocol



Diffie-Hellman protocol



Diffie-Hellman protocol