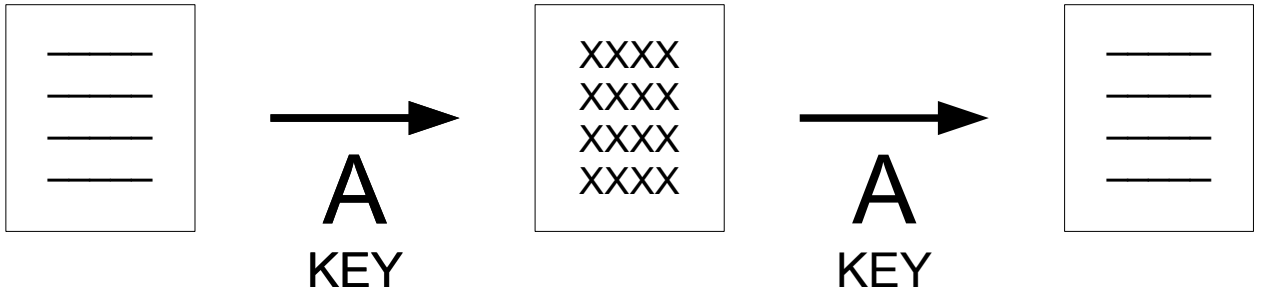
Vad man vill kunna göra

- Lagra och skicka krypterad information
- Säkerställa att information inte manipuleras
- Signera sådant som man står för

Teknik

- Symmetrisk kryptering
- Asymmetrisk kryptering
- Hashfunktioner

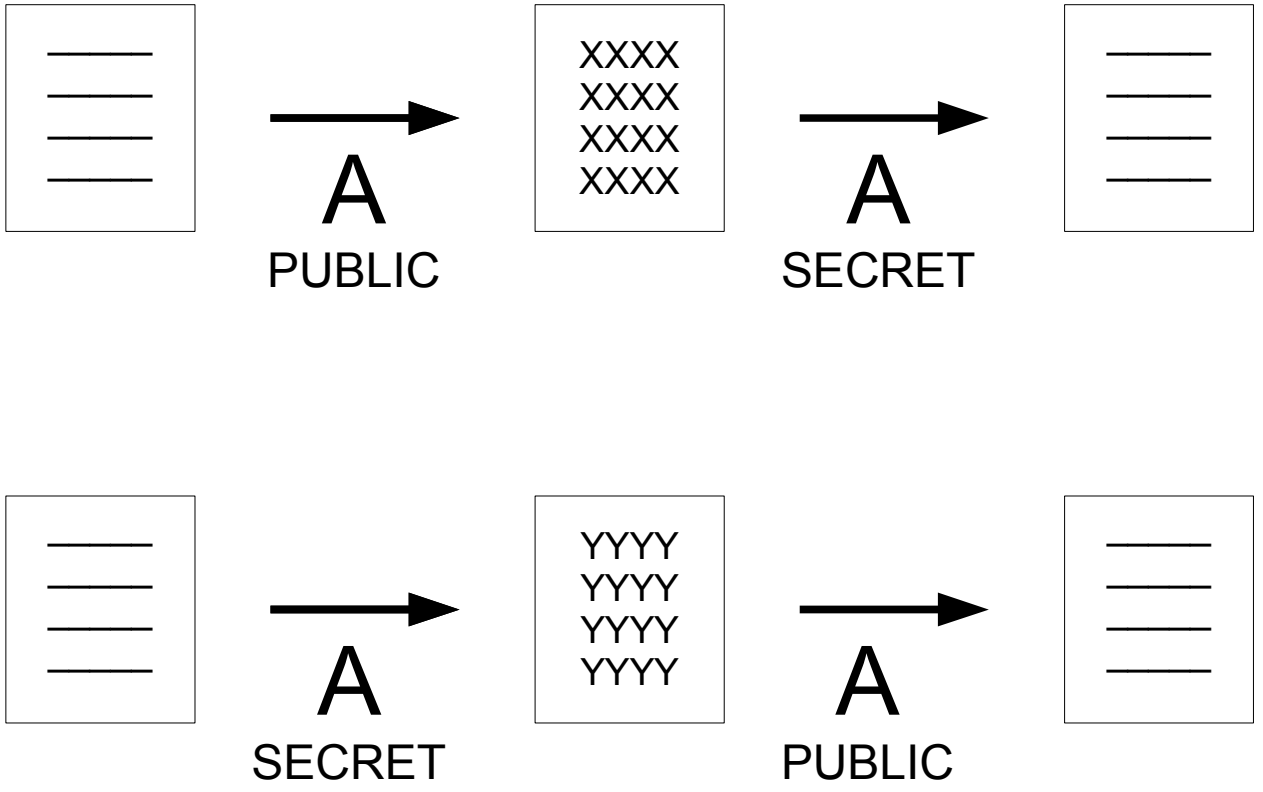
Symmetrisk kryptering



Symmetrisk kryptering

- Det finns **en nyckel** som använd både för kryptering och dekryptering
- Snabb
- Extremt säker
- Normal nyckellängd idag är 128-256 bittar
- Advanced Encryption Standard (*AES*) är idag vanligast, men det finns andra, t.ex. *Blowfish* och den äldre *DES*

Asymmetrisk kryptering



Asymmetrisk kryptering

- Det finns **två nycklar** som genererats tillsammans, en **publik** som du publicerar eller lämnar ut till dem som ska skicka meddelanden till dig, och en som man håller **hemlig**.
- Meddelanden kan krypteras med den **publika** nyckeln och kräver då den **hemliga** nyckeln för att dekrypteras (den publika nyckeln kan inte användas för att dekryptera meddelandet)
- Meddelanden kan också krypteras med den **hemliga** nyckeln och kräver då den **publika** nyckeln för att dekrypteras (den hemliga nyckeln kan inte användas för att dekryptera meddelandet)

Asymmetrisk kryptering

- Ganska långsam
- Har svagheter som gör att den går att angripa om innehållet i ett meddelande är känt
- Kräver *padding*, gör att alla meddelanden blir större
- Normal nyckelängd idag är 1024-2048 bittar
- *RSA* och *el Gamal* är de mest kända algoritmerna

Värdet med asymmetrisk kryptering

- **Kryptering utan distribution av hemliga nycklar** – Vem som helst kan skicka krypterade meddelanden till mig utan att vi behöver dela på en hemlighet i förväg
- **Signering** – Om jag skickar ut ett meddelande som är krypterat med min hemliga nyckel så kan vem som helst läsa det och lita på att det är jag som har skrivit det. Det är ju bara jag som har nyckeln som krävs för kryptering.

Hashfunktioner

- Beräknar en typ av checksumma
- En bra hashfunktion ska generera väldigt olika checksummor för meddelanden som ser nästan likadana ut
- Det ska vara extremt svårt att skapa olika meddelanden som får samma hashvärde
- Exempel på moderna hashfunktioner är Secure Hash Algorithm (*SHA*)
- SHA finns i olika längder och varianter. SHA256 och SHA512 är rekommenderade idag, men nya varianter kommer

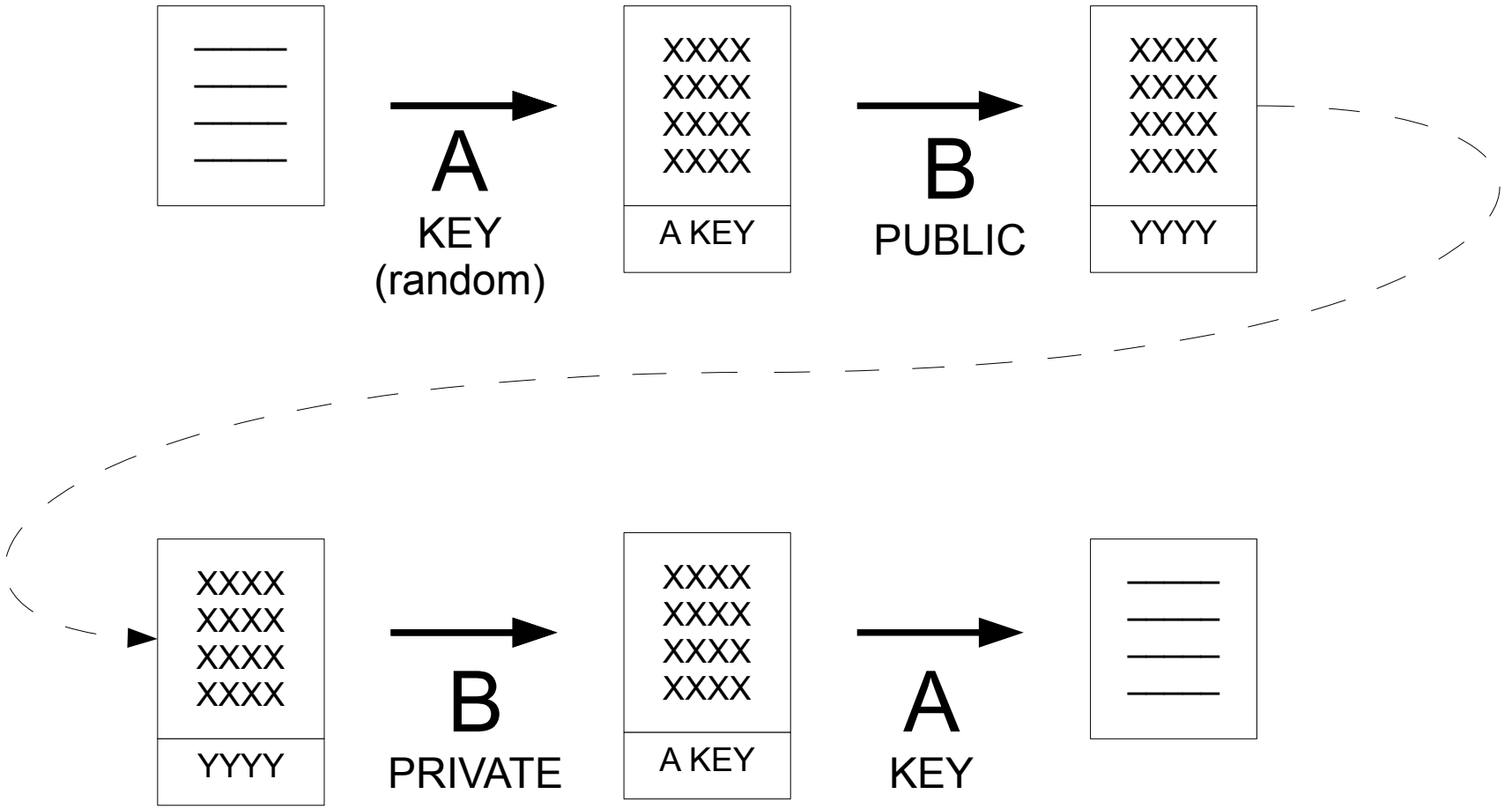
Värdet med hashfunktioner

- Man behöver inte signera hela texter och program
- Det räcker med att räkna hashvärdet på det man vill signera och sedan signera det

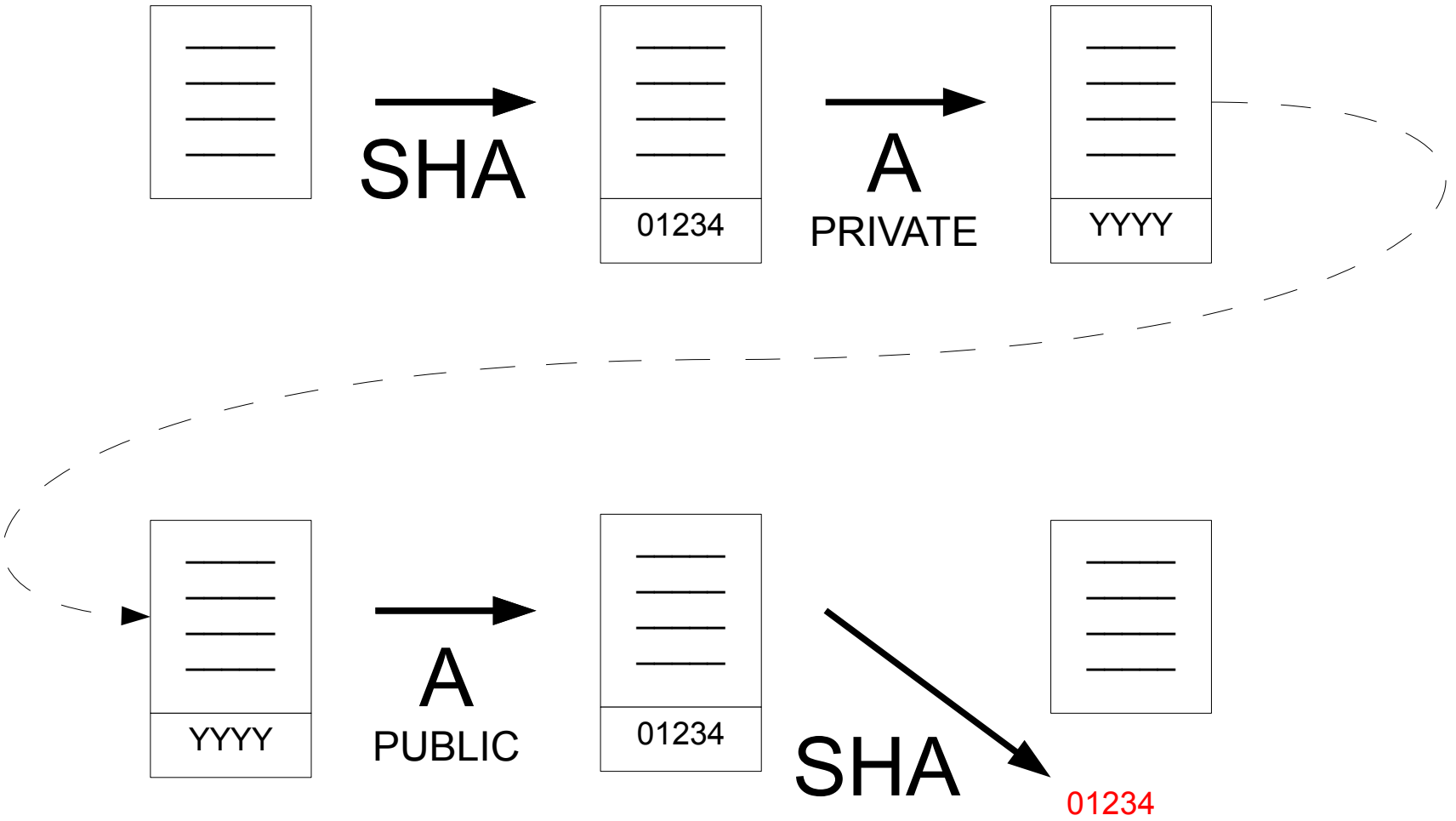
Hashexempel

```
$ sha256sum
Min hemliga text

2dd6d07119ac3ddfbd9603d52b87ccf97fa9043c52abc5be76279f9cbe5446b5  -

$ sha256sum
Min heliga text

12bf5ce01a85fc875550bf6a05a9e3240238f0e21aa66ac9cc184f5e99a234a4  -

$ sha256sum
Sed ut perspiciatis, unde omnis iste natus error sit voluptatem accusantium
 doloremque laudantium, totam rem aperiam eaque ipsa, quae ab illo inventore
 veritatis et quasi architecto beatae vitae dicta sunt, explicabo. Nemo enim
 ipsam voluptatem, quia voluptas sit, aspernatur aut odit aut fugit, sed quia
 consequuntur magni dolores eos, qui ratione voluptatem sequi nesciunt, neque
 porro quisquam est, qui dolorem ipsum, quia dolor sit amet, consectetur,
 adipisci[ng] velit, sed quia non numquam [do] eius modi tempora inci[di]dunt,
 ut labore et dolore magnam aliquam quaerat voluptatem.

17de33af8ae231236b8a157fe3f507a6581a8697190fd86e59f09086cabab673  -
```

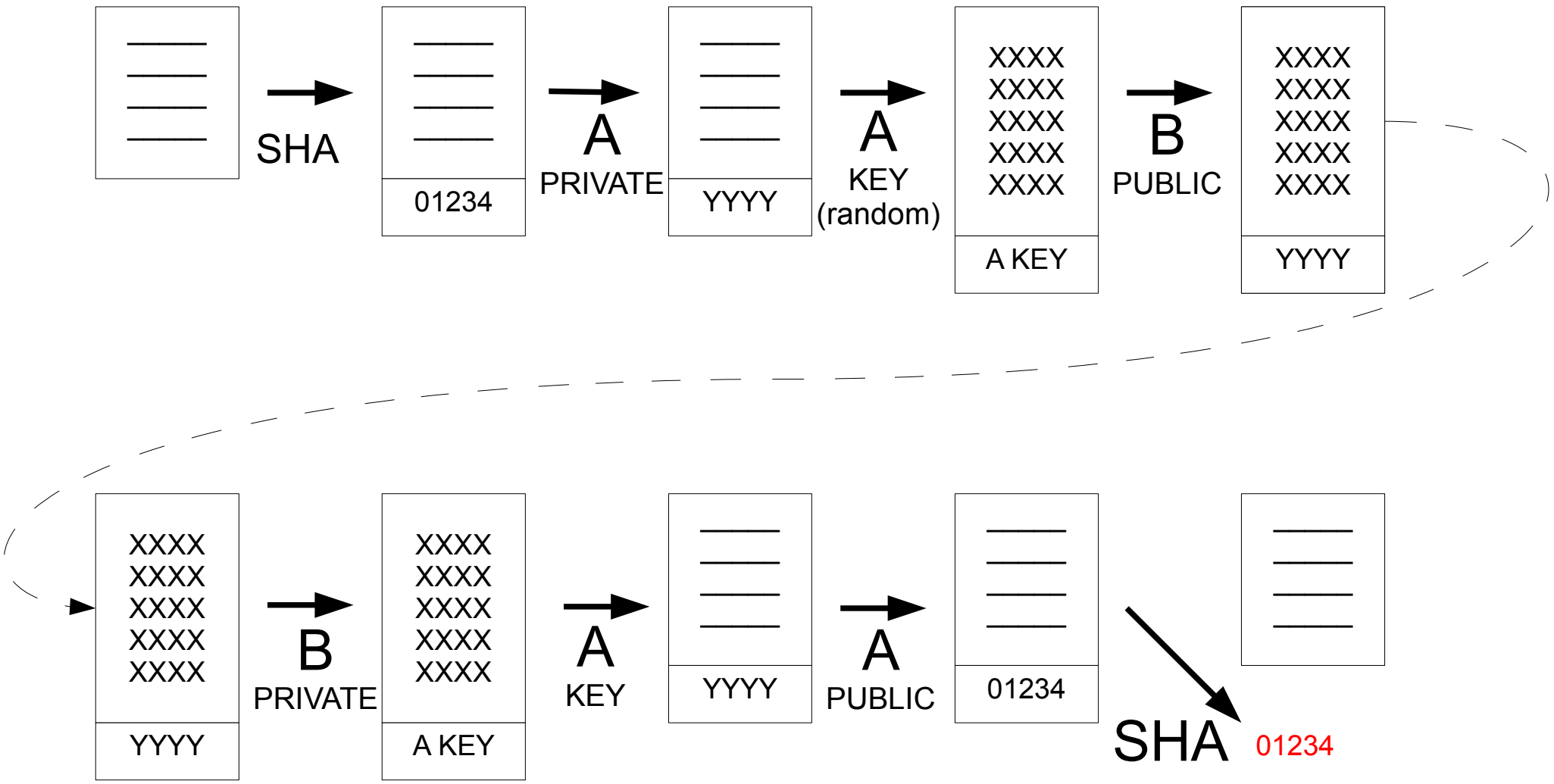
Krypterat brev från A till B



Signerat brev från A till B



Signerat krypterat brev från A till B



Certifikat

- En pålitlig tredje part signerar din publika nyckel med sin hemliga nyckel
- Det gör att andra som litar på den tredje parten kan lita på att din publika nyckel är din, eftersom de kan använda tredjepartens publika nyckel för verifikation
- Webläsare har en lista med tredjeparter som leverantören betraktar som pålitliga
- Leverantörerna tar betalt för att utfärda certifikat
- Litar du på dem?

Web of trust

- I stället för att lita på certifikatutfärdare kan man bygga nätverk där var och en kan bestämma vem man litar på
- Detta görs genom att man låter alla signera vilka nycklar de vill. Man kan då spåra en publik nyckel och se om man litar på den kedja som leder till en själv.
- Signering görs ofta vid ”signing parties”, där folk visar upp sina nycklar och sin legitimation
- Signerade nycklar läggs vanligen upp i publika nyckelringar
- Öppen Källkod-rörelsen arbetar ofta med *Web of Trust*