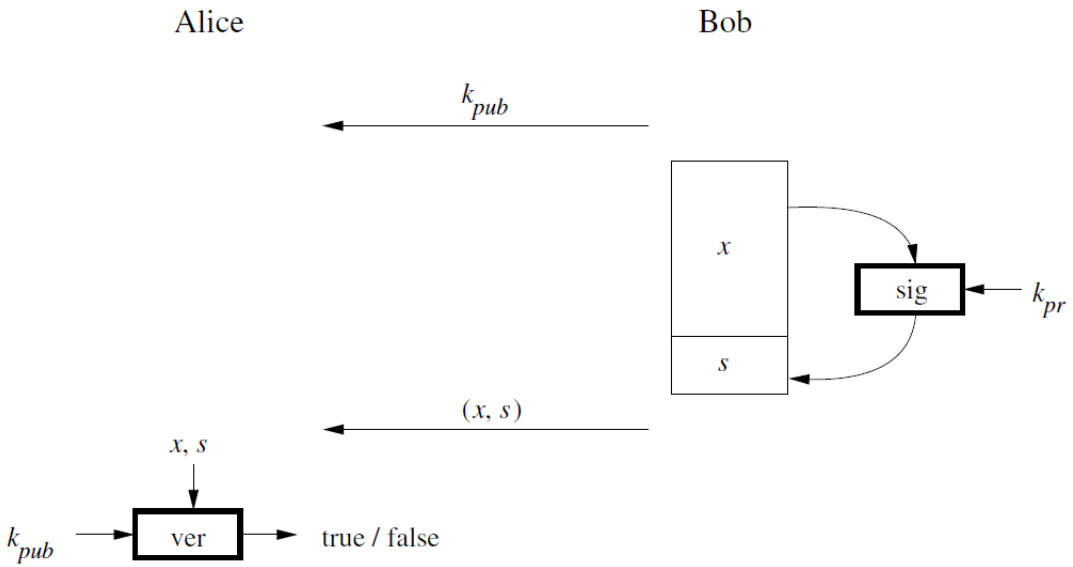
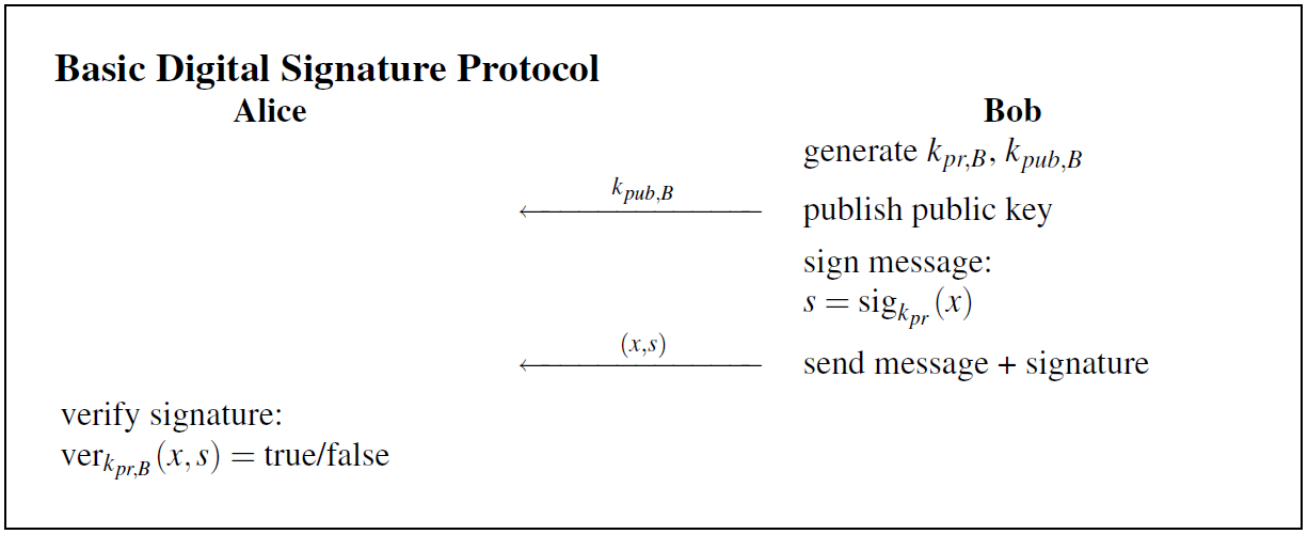
امضاهای دیجیتالی

- فرآیند
  - امضای پیام
  - درستی‌سنجی امضا



امضاهای دیجیتالی

- پروتکل پایه



طرح امضای RSA

- تولید کلید
  - هر کاربر یک زوج کلید خصوصی/عمومی تولید می‌کند
    - انتخاب دو عدد اول بزرگ p و qبه صورت تصادفی
    - محاسبه $n = pq$
      - $\varphi(n) = (p-1)(q-1)$
    - انتخاب کلید رمزگذاری e به گونه‌ای که $gcd(\varphi(n),e) = 1$ و $1 < e < \varphi(n)$
    - محاسبه کلید رمزگشایی d به گونه‌ای که $d \equiv e^{-1} \pmod{\varphi(n)}$
      - الگوریتم گسترش یافته اقلیدس
    - کلید خصوصی
      - $PR = d$
    - کلید عمومی
      - $PU = (e,n)$

طرح امضای RSA

- پروتکل امضای دیجیتالی پایه

Basic RSA Digital Signature Protocol

Alice		Bob
		$k_{pr} = d, k_{pub} = (n, e)$
	$\xleftarrow{(n,e)}$	
		compute signature: $s = \text{sig}_{k_{pr}}(x) \equiv x^d \bmod n$
	$\xleftarrow{(x,s)}$	

verify: $\text{ver}_{k_{pub}}(x, s)$

$x' \equiv s^e \bmod n$

$$x' \begin{cases} \equiv x \bmod n & \Longrightarrow \text{valid signature} \\ \not\equiv x \bmod n & \Longrightarrow \text{invalid signature} \end{cases}$$

طرح امضای RSA

- مثال

Alice

Bob

1. choose $p = 3$ and $q = 11$
2. $n = p \cdot q = 33$
3. $\Phi(n) = (3-1)(11-1) = 20$
4. choose $e = 3$
5. $d \equiv e^{-1} \equiv 7 \bmod 20$

$(n,e)=(33,3)$ ←

compute signature for message $x = 4$:
$s = x^d \equiv 4^7 \equiv 16 \bmod 33$

$(x,s)=(4,16)$ ←

verify:
$x' = s^e \equiv 16^3 \equiv 4 \bmod 33$
$x' \equiv x \bmod 33 \Longrightarrow$ valid signature

طرح امضای RSA

- انواع حمله‌ها
  - حمله‌های الگوریتمی
    - تجزیه پیمانه n به عوامل اول p و q
  - Existential Forgery
    - تولید یک امضای معتبر برای یک پیام تصادفی x

طرح امضای RSA

- **Existential Forgery**

Existential Forgery Attack Against RSA Digital Signature

Alice	Oscar	Bob
		$k_{pr} = d$ $k_{pub} = (n, e)$
	$\xleftarrow{(n,e)}$	$\xleftarrow{(n,e)}$
	1. choose signature: $s \in \mathbb{Z}_n$ 2. compute message: $x \equiv s^e \bmod n$	
	$\xleftarrow{(x,s)}$	

verification:
$s^e \equiv x' \bmod n$
since $x' = x$
$\Longrightarrow$ valid signature!

طرح امضای RSA-PSS