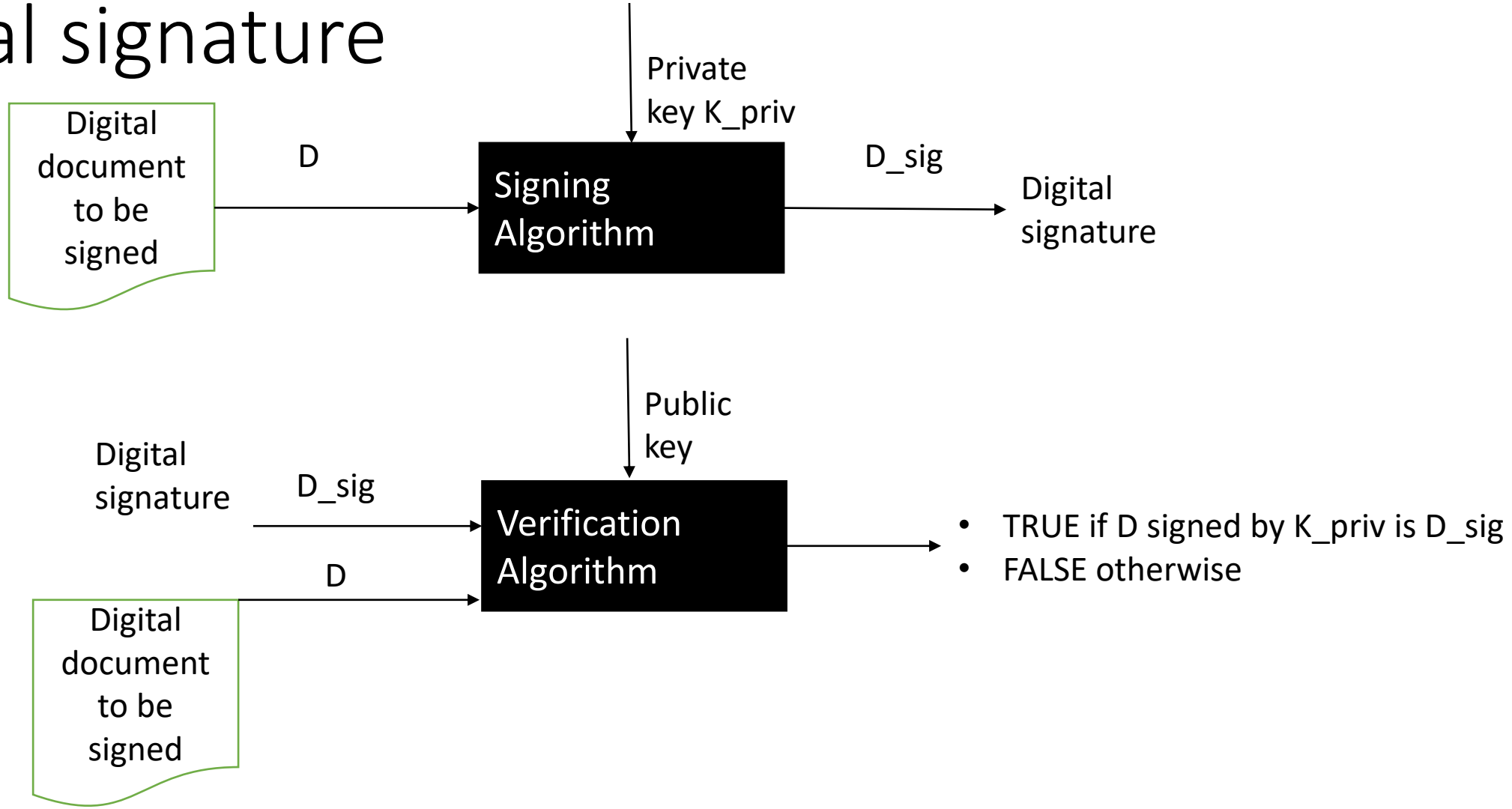
Advanced Cryptography

Lesson 5

Digital signature



RSA digital signature

Samantha **Victor**

Key Creation

Choose secrete primes p, q
Choose verification exponent v with
$\gcd(v, (p-1)(q-1)) = 1$
Publish N = pq and v

Signing

Compute s satisfying
$s \equiv 1 \pmod{(p-1)(q-1)}$
Sign document D by computing
$S \equiv D^s \pmod{N}$

Verification

Compute S_v mod N and
Verify that it is equal to D

Elliptic curves over F_2 and over F_2^k

Theorem (Hasse). With $E(F_p^k)$, $\#E(F_p^k) = p^k + 1 - t_p^k$ with t_p^k satisfying $|t_p^k| \leq 2p^{k/2}$.

#E$(F_2) = 5$, so $\#E(F_2)$ is not useful for cryptographic purposes.

Definition. An elliptic curve E is the set of solutions to a generalized Weierstrass equation (E): $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, together with an extra point O. the coefficients $a_1, \ldots, a_6$ are required to satisfy $\Delta \neq 0$, where the discriminant Δ is defined as follows:

- $b_2 = a_1^2 + 4a_2, b_2 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6,$
- $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$
- $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$

ElGamal digital signatures

Public Parameter Creation

A trusted party chooses and publishes a large prime p and primitive root g modulo p

Samatha **Victor**

Key creation

Choose secret signing key $1 \leq s \leq p - 1$.
Compute $v \equiv g^s \pmod{p}$.
Publish the verification key v.

Signing

Choose document D mod p.
Choose ephemeral key e mod p.
Compute signature
. $S_1 \equiv g^e \pmod{p}$.
. $S_2 \equiv (D - sS_1)e^{-1} \pmod{p-1}$

Verification

Compute $v^{S_1}S_1^{S_2} \bmod p$.
Verify that it is equal to $g^D \bmod p$.

DSA – digital signature algorithm

Public Parameter Creation

A trusted party chooses and publishes a large primes p and q satisfying $p \equiv 1 \pmod{q}$ and an element g of order q modulo p

Samatha **Victor**

Key creation

Choose secret signing key $1 \leq s \leq q - 1$.
Compute $v \equiv g^s \pmod{p}$.
Publish the verification key v.

Signing

Choose document D mod p.
Choose ephemeral key e mod p.
Compute signature
. $S_1 \equiv g^e \pmod{p}$.
. $S_2 \equiv (D + sS_1)e^{-1} \pmod{p-1}$

Verification

Compute $DS_1{}^{S}{}_2 \bmod p$ and $V_2 \equiv S_1 S_2{}^{-1} \pmod{q}$.
Verify that $(g^{V}{}_1 v^{V}{}_2 \bmod p) \bmod q = S_1$.