2550 Intro to cybersecurity

L8: Crypto: PKC

abhi shelat

Basic Number theory

$$a \bmod p$$

$17 \bmod 11 = 6$

$17 + 135433238 =$ 1

123121

11 $135433238 \bmod 11 = 6$

4
25
22
34
33
13
4
22
12

Basic number theory

Modular arithmetic

Claim 28.1. *For $n > 0$ and $a, b \in \mathbb{Z}$,*

1. $(a \bmod n) + (b \bmod n) = (a + b) \bmod n$

2. $(a \bmod n)(b \bmod n) \bmod n = ab \bmod n$

Modular Exponentiation

$(a, x, n) \to a^x \bmod n$

10011

$5^{19} \bmod 31$

powers:

1	2	4	8	16
5	25	625 mod 31 = 5	25	5

$$31 \overline{)625}$$

$$\begin{array}{r} 62 \\ \hline 05 \\ \hline \end{array}$$

$$5^{19} = 5^{16} \cdot 5^2 \cdot 5^1 = 5 \cdot 25 \cdot 5 = 5$$

$5^{1024195} \bmod 167$

$$5^{19} = (5^9)^2 \cdot 5$$

Modular Exponentiation

$$(a, x, n) \rightarrow a^x \bmod n$$

Algorithm 2: ModularExponentiation(a, x, n)

```
Input: a, x ∈ [1, n]
r ← 1
while x > 0 do
    if x is odd then
        r ← r · a mod n
    x ← ⌊x/2⌋
    a ← a² mod n
Return r
```

Modular Exponentiation

$$(a, x, n) \to a^x \bmod n$$

$$a^x \bmod n = \prod_{i=0}^{\ell} x_i a^{2^i} \bmod n$$

Algorithm 2: ModularExponentiation(a, x, n)

```
Input: a, x ∈ [1, n]
r ← 1
while x > 0 do
    if x is odd then
        r ← r · a mod n
    x ← ⌊x/2⌋
    a ← a^2 mod n
Return r
```

Greatest Common Divisor

EUCLID

$$\mathrm{GCD}(\underline{A}, \underline{B}) = \mathrm{GCD}(B, A \bmod B)$$

Greatest Common Divisor

$\mathrm{GCD}(6809, 1639) = \mathrm{GCD}(1639, \underbrace{6809 \bmod 1639}_{253})$

$= \mathrm{GCD}(253, \underbrace{1639 \bmod 253}_{121})$

$= \mathrm{GCD}(121, \underbrace{253 \bmod 121}_{11})$

$= \mathrm{GCD}(11, 121 \bmod 11) = \boxed{11}, 0$

given (a,b), finds (x,y) s.t.

ax + by = gcd(a,b)

Algorithm 1: ExtendedEuclid(a, b)

Input: (a, b) s.t $a > b \geq 0$

Output: (x, y) s.t. $ax + by = \gcd(a, b)$

if $a \bmod b = 0$ **then**

  Return $(0, 1)$

else

  $(x, y) \leftarrow \texttt{ExtendedEuclid}\,(b, a \bmod b)$

  Return $(y, x - y(\lfloor a/b \rfloor))$

---

groups

$(G, \oplus)$

set of numbers or other elements $\{0, 1, 2, \ldots, 6\}$

$\oplus$ → operation between 2 elements

closure – if $a, b \in G$, then $a \oplus b \in G$.

associativity → $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

identity – $\exists\, i \in G$ s.t. $\forall a \in G$ $a \oplus i = a$

inverse → $\forall a \in G$, $\exists\, a^{-1} \in G$ s.t. $a^{-1} \oplus a = i$

example of groups

$$(\mathbb{Z}_n, +)$$

Example of groups

pos.
all integers that are relatively prime to n.

$$(\underbrace{\mathbb{Z}_n, \star}) \qquad \{a \mid \gcd(a,n)=1\} \qquad \mathbb{Z}_n^\star$$

multiplicative group, mod n

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$*$: multiplication mod n.

$3 \cdot 5 = 15 \bmod 7 = 1$

closure,
associativity
identity:
inverses: ✓

Extended Euclid.

$\gcd(a,n)=1.$

$\Rightarrow \exists x, y \quad a \cdot x + y \cdot n = 1$

$\Rightarrow \quad a \cdot x \bmod n = 1$

Euler totient

$\varphi(n) = \#$ of positive integers up to n that are relatively prime to n.

$\varphi(7) = |\mathbb{Z}_7^*| = |\{1,2,3,4,5,6\}| = 6$

$\varphi(p) = p - 1$ → p is a prime

$\varphi(15) = |\{1, 2, 4, 7, 8, 11, 13, 14\}|$

$= 15 = 3 \cdot 5$

$$\boxed{\varphi(15) = (3-1)(5-1) = 2 \cdot 4 = 8}$$

3 6 9 12 5 10 15

Euler theorem

$\varphi(n) \rightarrow$ totient function

$$\forall a \in \mathbb{Z}_n^\star,\ a^{\Phi(n)} = 1 \bmod n$$

$4 \in \mathbb{Z}_{15}^*$.

$4^8 \equiv 1 \bmod 15.$

$7^8 \equiv 1 \bmod 15.$

1	2	4	8
4	1	1	1
7	4	1	1

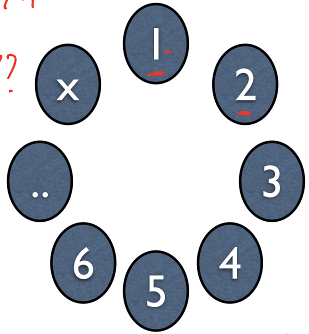
Euler theorem

$= \phi(N)$

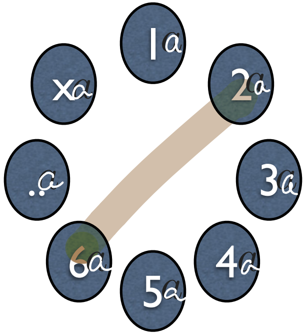
$$\forall a \in \boxed{\mathbb{Z}_N^\star},\ a^{\Phi(N)} = 1 \bmod N$$

how many in this circle?? $\rightarrow$

$\phi(N)$



same set of numbers $\longleftrightarrow$



$\leftarrow$ this circle has the same set of numbers as the left one.

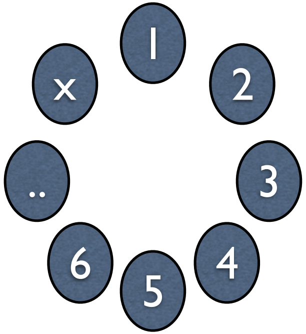
why?? Suppose 2 are the same, say these 2.

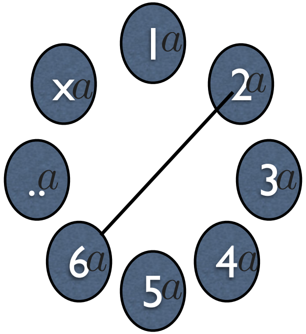
$2a = 6a \Longrightarrow$ mult by a^{-1}

$2a \cdot a^{-1} = 6a \cdot a^{-1} \Rightarrow 2 = 6$ ☒ contradiction!!

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$





argue: all are distinct

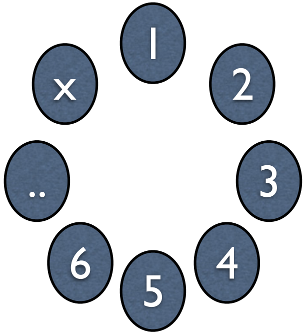
spse two are equal.

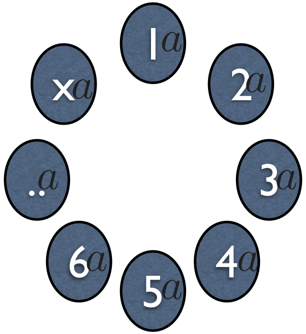
multiply by a^{-1}

this implies 2=6!

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$





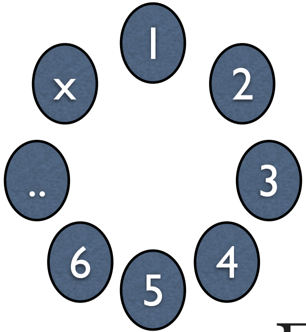
product

$$\prod_{x \in \mathbb{Z}_n^*} x = \prod_{x \in \mathbb{Z}_n^*} a x$$

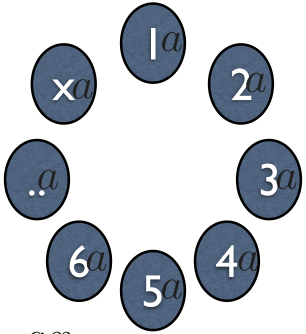
$$\cancel{\prod x} = a^{\varphi(n)} \cdot \cancel{\prod x} \Longrightarrow 1 \equiv a^{\varphi(n)} \bmod N.$$

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$



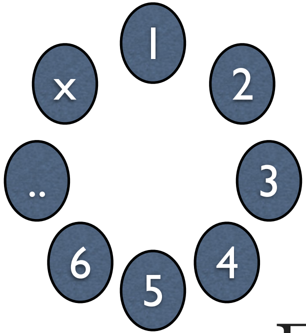
$$\prod_{x \in Z_N^\star} x$$

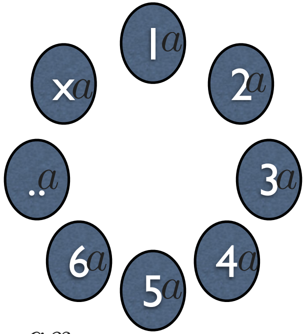


$$\prod_{x \in Z_N^\star} ax$$

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$

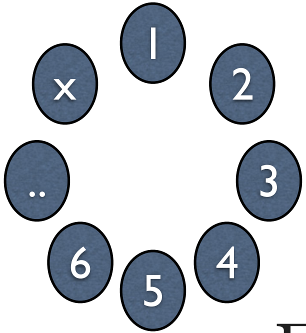


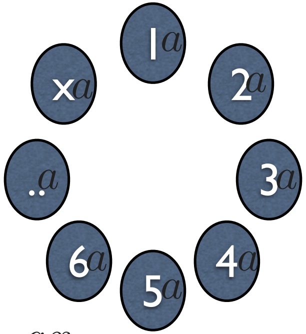


$$\prod_{x\in Z_N^\star} x = \prod_{x\in Z_N^\star} ax$$

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$



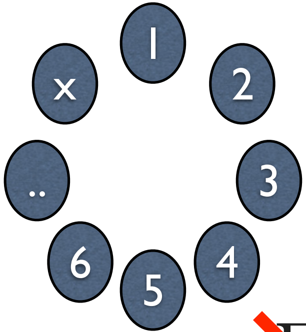


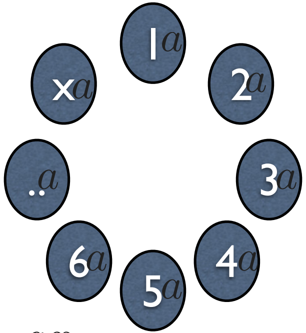
$$\prod_{x \in Z_N^\star} x = \prod_{x \in Z_N^\star} ax$$

$$a^{\Phi(N)} \prod_{x \in Z_N^\star} x$$

Euler theorem

$$\forall a \in \mathbb{Z}_N^\star,\ a^{\Phi(N)} = 1 \bmod N$$





$$\cancel{\prod_{x\in Z_N^\star}} x = \prod_{x\in Z_N^\star} ax$$

$$a^{\Phi(N)} \cancel{\prod_{x\in Z_N^\star}} x$$

compute $$11^{31^{2020}} \bmod 23$$ (show your work)

mod equivalence

$\varphi(23) = 22$

$11^{31^{2020}} \bmod 23 = 11^{\underbrace{31^{2020}}} \bmod 23$

$31^{2020} \bmod 22$

$11^{22} \equiv 1$

E.T.

$31^{2020} \bmod 22 = \boxed{31^{2020 \bmod 10}} \bmod 22 = (31^{10})^{202} \bmod 22$

$\varphi(22) = (2-1)(11-1) = 10 \Rightarrow 31^{10} \equiv 1 \bmod 22$

$11^{22} = 1 \bmod 23$

$2020 \bmod 10 = \underline{0}$

$11^{\varphi(23)} = 1 \bmod 23$

$1^{202} \bmod 22 = 1.$

$\Rightarrow 11^{31^{2020}} \bmod 23 = 11^{1} \bmod 23 = \boxed{11}$

El-Gamal encryption

(sk, pk)

prime of size n bits.

gen(1^n)

$p \leftarrow \Pi_n \quad g \leftarrow \text{Generators}_p$

$sk \leftarrow \{1 \ldots p-1\} \in \mathbb{Z}_p^*$ $\quad pk = g^{sk} \bmod p.$

enc$_{pk}$(m)

$r \leftarrow \mathbb{Z}_p^*.$

$c_0 = g^r \bmod p \qquad c_1 = (pk)^r \cdot m \bmod p.$

dec$_{sk}$(c)

$c_1 \cdot \underbrace{(c_0^{sk})^{-1}}_{} \bmod p.$

El-Gamal encryption

gen(1^n)

$$p \leftarrow \Pi_n \quad g \leftarrow \text{Generators}_p$$

$$a \leftarrow \mathbb{Z}_p$$

$$pk \leftarrow (g, g^a) \quad sk \leftarrow (g, a)$$

enc$_{pk}$(m)

$$r \leftarrow \mathbb{Z}_p$$

$$(g^r, (g^a)^r \cdot m)$$

dec$_{sk}$(c)

$$(c_1, c_2) \leftarrow c$$

$$m \leftarrow c_2/(c_1)^a$$

Example ElGamal

$pk \leftarrow (g, g^a) \quad sk \leftarrow (g, a)$

enc$_{pk}$(m)

$r \leftarrow \mathbb{Z}_p$

$c \leftarrow g^r, pk^r \cdot m$

dec$_{sk}$(c)

$(c_1, c_2) \leftarrow c$

$m \leftarrow c_2/(c_1)^a$

msg=“ “

Example

Why it works: $pk = g^{sk}$

$c_1 = pk^r \cdot m = (g^{sk})^r \cdot msg = (g^r)^{sk} \cdot msg$

$= (c_0)^{sk} \cdot msg$

Why is ElGamal secure?

decisional Diffie-Hellman assumption (DDH)

$p \leftarrow \Pi_n \quad g \leftarrow \text{Generators}_p$

$a, b, c \leftarrow \mathbb{Z}_p$ (work in a prime order group)

$$\{p, g, g^a, g^b, g^{ab}\}_n \approx \{p, g, g^a, g^b, g^c\}_n$$

$g^{sk}, g^r, g^{sk \cdot r}$ $\qquad$ g^{sk}, g^r, g^c

“Textbook” RSA (insecure)

- Pick N = p*q where p,q are primes.
- Pick e,d such that $e \cdot d = 1 \mod \phi(N)$
- $\text{Enc}_{N,e}(m) = m^e \mod N$

  $\text{Dec}_{N,d}(c) = c^d \mod N$

Euler's theorem

$$\underbrace{(m^e)}_{\text{Enc}}{}^d \mod N = m^{ed} \mod N = m^1 \mod N = m$$

Dec

“Textbook” RSA (insecure) Example

Pick N = p*q where p,q are primes.

$\overset{p}{11} * \overset{q}{13}$: N=11*13 = 143

Pick e,d such that $e \cdot d = 1 \mod \phi(N)$

$\varphi(N) = (11-1)(13-1) = 120.$

$\text{Enc}_{N,e}(m) = m^e \mod N$

$e = 7 \quad d = 103$

$\text{Dec}_{N,d}(c) = c^d \mod N$

$m = 5$

$enc(5) = 5^7 \bmod 143.$

$= 47.$

$Dec(47^{103} \bmod 143) = 5. \bmod 143$

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \mod \phi(N)$

$\text{Enc}_{N,e}(m) = m^e \mod N$

$\text{Dec}_{N,d}(c) = c^d \mod N$

Why is it insecure against IND-CPA attack?

pkcs1.5

$\text{enc}_{pk}(m)$

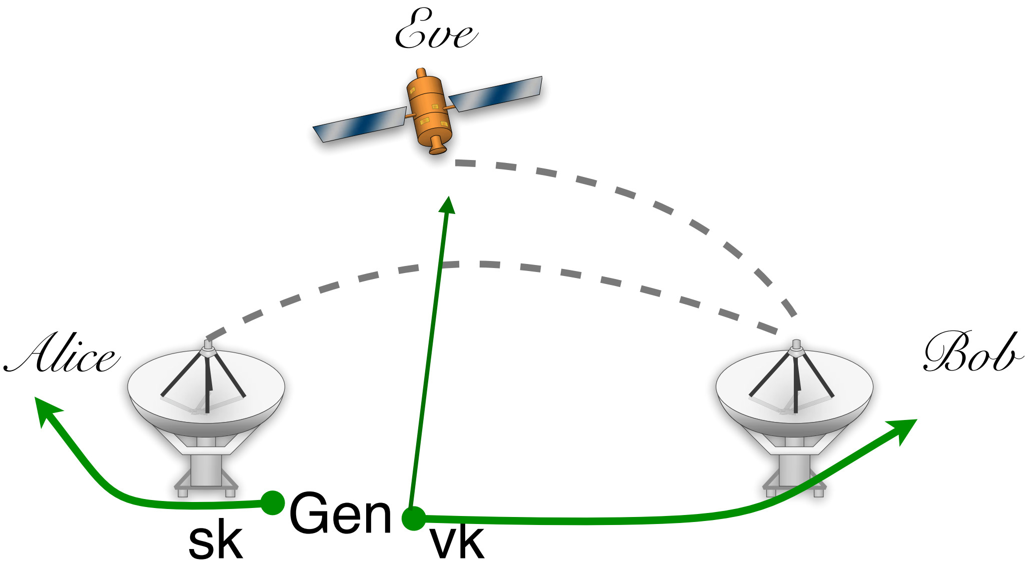
pick r as a random string with no 0s

(typically 8 bytes)

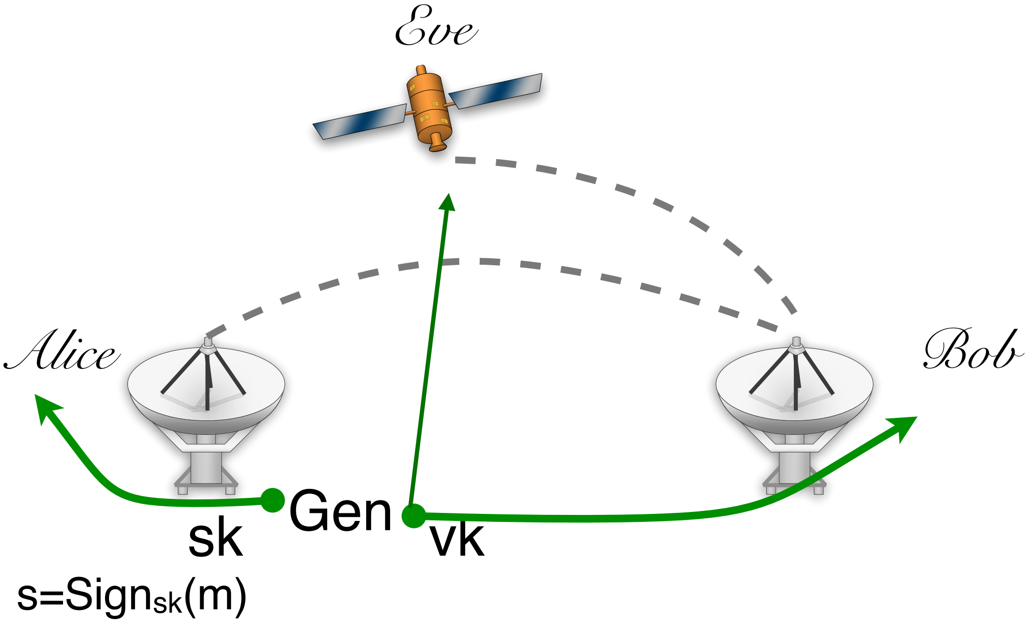
$$c \leftarrow (0||2||r||0||m)^e \bmod N$$

“padding oracle” attack against this scheme

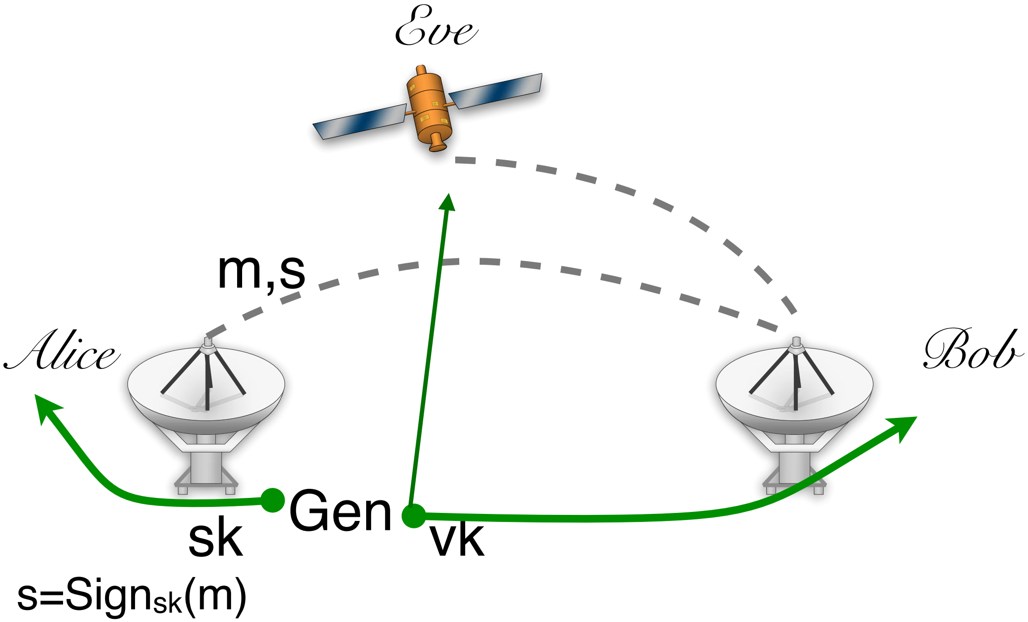
Public key digital signature



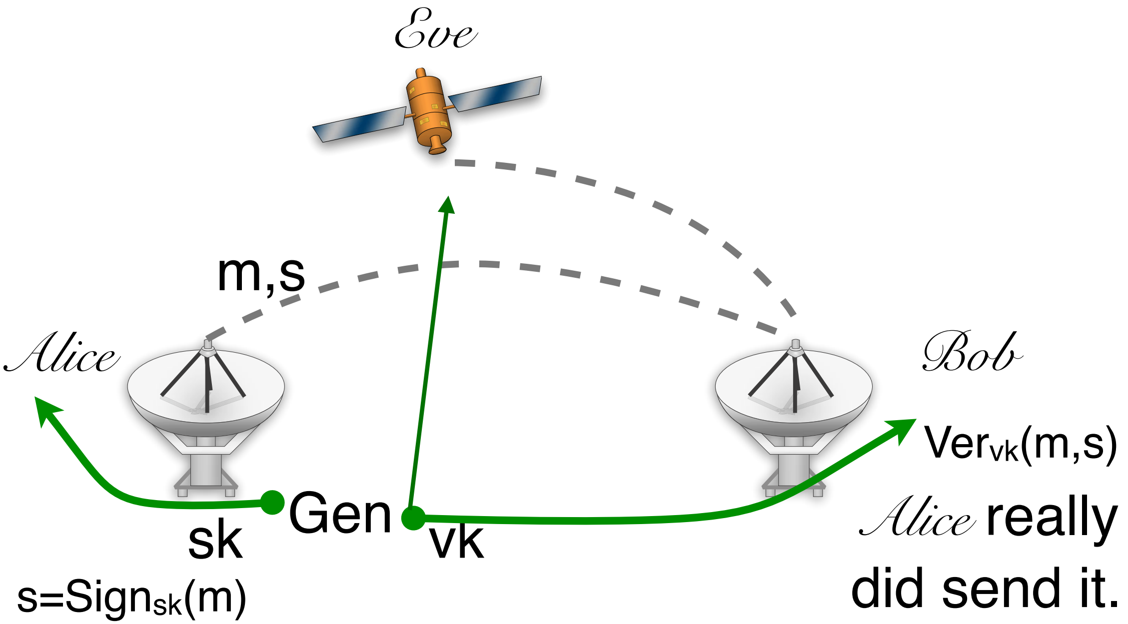
Public key digital signature



Public key digital signature



Public key digital signature



Public key digital signature

message space $\{\mathcal{M}\}_n$

$\mathrm{Gen}(1^n)$

$\mathrm{Sign}_{sk}(m)$

$\mathrm{Ver}_{vk}(m,s)$

Public key digital signature

message space $\{\mathcal{M}\}_n$

$\mathrm{Gen}(1^n)$ generates a key pair sk,vk

$\mathrm{Sign}_{sk}(m)$

$\mathrm{Ver}_{vk}(m,s)$

Public key digital signature

message space $\{\mathcal{M}\}_n$

$\mathrm{Gen}(1^n)$ generates a key pair sk,vk

$\mathrm{Sign}_{sk}(m)$ generates a signature s for $m \in \mathcal{M}_n$

$\mathrm{Ver}_{vk}(m,s)$

Public key digital signature

message space $\{\mathcal{M}\}_n$

$\text{Gen}(1^n)$ generates a key pair sk,vk

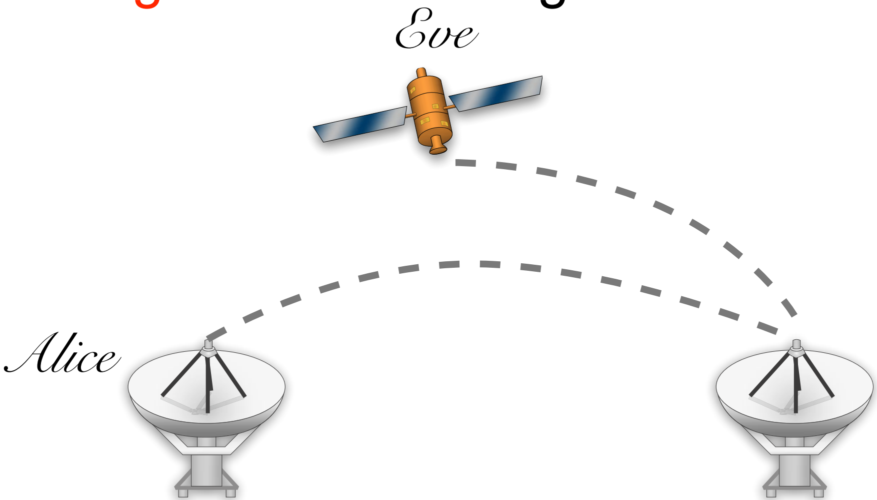
$\text{Sign}_{sk}(m)$ generates a signature s for $m \in \mathcal{M}_n$

$\text{Ver}_{vk}(m,s)$ accepts or rejects a msg,sig pair

$$\Pr[k \leftarrow Gen(1^n) : Ver_{vk}(m, Sign_{sk}(m)) = 1] = 1$$

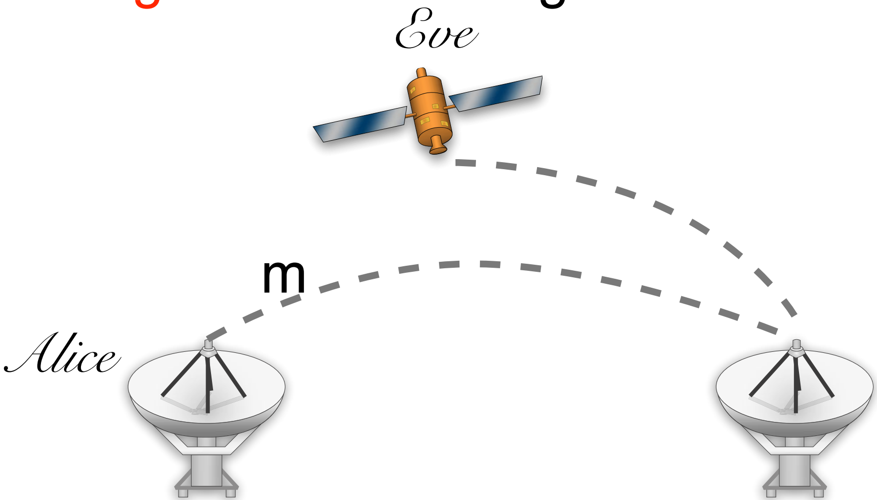
existential unforgability

“even when given a signing oracle,
an adversary cannot forge a signature for
any message of its choosing ”



existential unforgability

"even when given a signing oracle,
an adversary cannot forge a signature for
any message of its choosing "



for all non-uniform ppt A

$$\Pr\Big[\qquad\qquad\qquad\qquad\qquad\qquad \Big] < \mu(n)$$

for all non-uniform ppt A

$$\Pr\left[\begin{array}{l}(vk, sk) \leftarrow Gen(1^n); (m, s) \leftarrow A^{Sign_{sk}(\cdot)} : \\ \quad Ver_{vk}(m, s) = 1 \\ \quad \text{and A didn't query m}\end{array}\right] < \mu(n)$$

Textbook RSA Signatures (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

Sign((sk=d, N) m):

Compute the signature: $\sigma \leftarrow m^d \bmod N$

Verify((pk=e, N), σ, m):

$$m \stackrel{?}{=} \sigma^e \bmod N$$

RSA Signatures in GPG

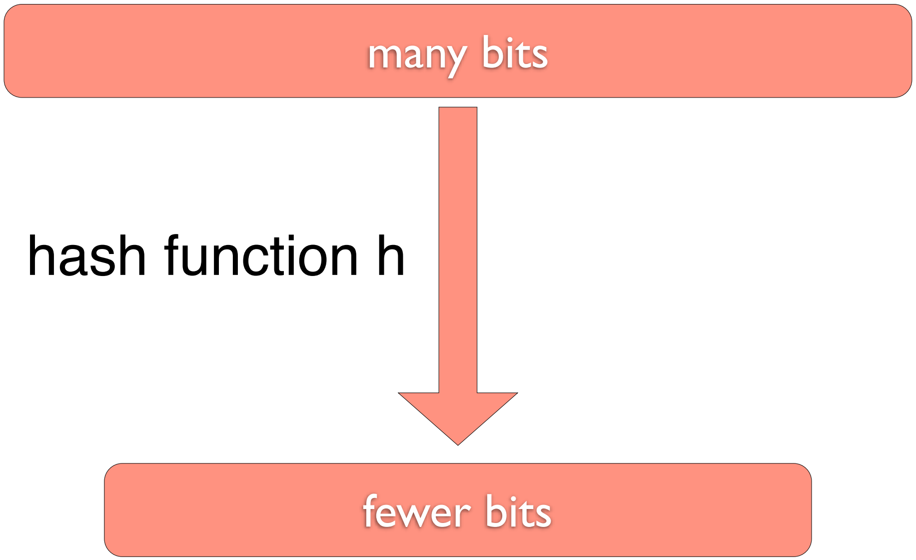
Sign((sk, N) m):

Compute the padding: $z \leftarrow 00 \cdot 01 \cdot FF \cdots FF \cdot 00 \cdot \mathsf{ID}_H \cdot H(m)$

Compute the signature: $\sigma \leftarrow z^{sk} \bmod N$

What is this H() function?

goal of a hash function



a hash function is a function

$$h : \{0,1\}^d \longrightarrow \{0,1\}^r$$

such that h is easy to evaluate
and r < d

useful in data structures

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785
```

collisions should be rare

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785

abhi$ java test “hello world”
1794106052
```

java hash function

$$h(s) = \sum_{i=0}^{n} s[i] 31^{n-i}$$

java hash function

$$h(s) = \sum_{i=0}^{n} s[i]31^{n-i}$$

it is thus easy to find a pair s_1, s_2
such that $h(s_1) = h(s_2)$

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785
```

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHGGGCc
-1644493785
```

```
public class test
{
    public static void main(String[] args)
    {
        System.out.println(args[0].hashCode());
    }
}
```

```
abhi$ java test HHHHHHHHHHHHHHHHHHHHGGGDD
-1644493785

abhi$ java test HHHHHHHHHHHHHHHHHHHHGGGCc
-1644493785
```

‘D’ - ‘c’ + 31(‘D’-‘C’) = 0

Collision resistant hash function

in addition to being easy to compute,
it should be “hard” for a p.p.t. adversary
to find a hash collision.

md4	1990
md5	1992
sha1	1994
sha256	2005
Sha3	2015

md4	1990	128 bit
md5	1992	128 bit
sha1	1994	160 bit
sha256	2005	256 bit
Sha3	2015	

md4	1990	128 bit	1995
md5	1992	128 bit	1998
sha1	1994	160 bit	2005*
sha256	2005	256 bit	
Sha3	2015		

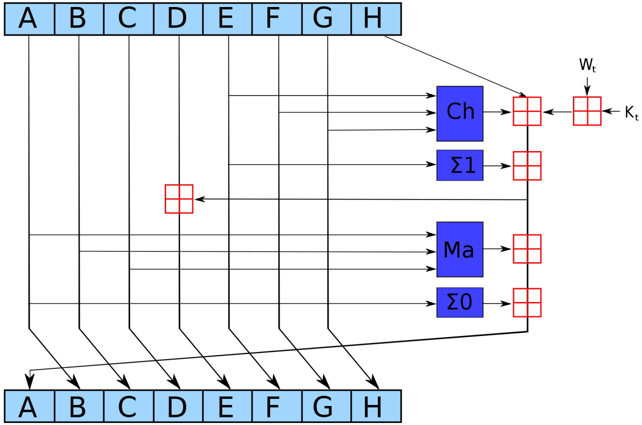
```
abhi18:neu abhi$ shasum -a 256
Noble patricians, patrons of my right,
Defend the justice of my cause with arms.
0c3c007b97cf8b75cfbd717804414a6a79b2defb4400eca9ea764a531a9ff193  -
```

Sha256

Pre-process the input

Break input into chunks

For each “chunk”, repeat this 64 times:



Most cryptographers consider SHA256 to be indistinguishable from a "Random oracle", i.e., a random function on arbitrary length messages.

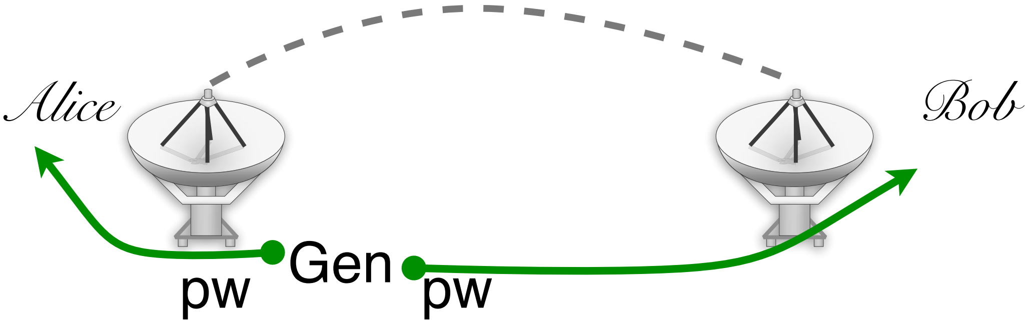
Recap:

Passwords

Main problem:

Passwords

Main problem:



Natural authenticators