Lecture notes Cryptology 2015

Thom Wiggers

September 26, 2015

1 Lecture 1 and 2

Cryptology consists of cryptography (constructive) and cryptanalysis (destructive).

1.1 Modular arithmetic

$\mathbb{Z}$ is the integers $\{\dots, -1, 0, 1, \dots\}$.

$\mathbb{Z}/n$ is the residue class of $\mathbb{Z}$ modulo n.

$$\mathbb{Z}/6 = \{0, 1, 2, 3, 4, 5, 6\} = \{-2, -1, 0, 1, 2, 3\}$$

We use integers to represent classes, so 0 stands for the set of integers congruent to $0 \mod 6$, i.e., $\{0, 6, 12, 18, \dots, -6, -12, \dots\}$.

$7 \equiv 1 \pmod 6$ ($\hat{=}7$ is congruent to $1 \pmod 6$).

We usually want the samllest representative on the right, depends on the set chosen, e.g. $17 \equiv 5 \equiv -1 \mod 6$.

1.2 Multiply mod n

When computing $a \cdot b \mod n$ we can compute and then reduce or reduce at any intermediate step.

$$17 \cdot 35 \equiv -1 \cdot -1 \equiv 1 \pmod 6$$

This is especially important for exponentiation $a^b \pmod n$.

1.2.1 Square and multiply

```
c = a
l = length of b as binary string
for i in reversed(range(l-2)):
  c = c^2 mod n
  if b_i == 1:
    c = c * a mod n
return c
```

1.3 Inverse mod n

Divide equation mod 7 by 4, this means undoing a multiplication by 4, i.e. find an integer mod 7 such that $a \cdot 4 \equiv 1 \pmod 7 = a^{-1} \equiv 4 \pmod 7$. Here $a \equiv 2 \pmod 7$ ($2 \cdot 4 \equiv 8 \equiv 1 \pmod 7$).

In general, use the Extended Euclidian Algorithm (xgcd) to compute a.

$$\text{xgcd}(n, m) = \begin{cases} \text{xgcd}(m, n) & m > n \\ \langle 1, 0 \rangle & n \mod m = 0 \\ \langle y, x - (y \cdot (n \operatorname{div} m)) \rangle & \langle x, y \rangle = \text{xgcd}(m, n \mod m) \end{cases}$$

See 1.6 for an example how to write this.

Inverses do not exist if the numbers are not coprime, e.g. 4 is not invertible mod 6 (common factor 2).

The set of invertible integers mod n is denoted $(\mathbb{Z}_{/n})^\times$. Example: $(\mathbb{Z}_{/7})^\times = \{1,2,3,4,5,6\}$, with inverses: $1^{-1} \equiv 1$, $2^{-1} \equiv 4$, $3^{-1} \equiv 5$, $6^{-1} \equiv 6$. These are exactly the integers coprime 7.

$(\mathbb{Z}_{/6})^\times = \{1,5\}$.

$(\mathbb{Z}_{/p})^\times = \{1,2,\ldots,p-1\}$ for p prime.

Eulers phi gives the size of $|(\mathbb{Z}_{/n})^\times| = \phi(n)$.

$\phi(7) = 6, \phi(6) = 2$.

$$\phi(p) = p - 1 \text{ for } p \text{ prime}$$

$$\phi(pq) = (p-1)(q-1) \text{ for } p, q \text{ prime}$$

$$\phi(p^b) = p^b - p^{b-1}$$

$$n = \prod_{i=0}^{l-1} p_i^{e_i}, p_i \neq p_j \text{ then } \phi(n) = \prod (p_i^{e_i} - p_i^{e_i - 1})$$

1.4 Lagrange's Theorem

Let G be a finite group of size $|G| = l$ then for any element $a \in G$ we have $a^l = 1$, where 1 is the neutral element and G is written multiplicatively.

eg. $a^6 \equiv 1 \pmod 7$ for $a \in (\mathbb{Z}_{/7})^\times$.

1.5 RSA

Pick two large primes p, q, with $p \neq q$. Put $n = pq$ and compute $\phi(n) = (p-1)(q-1)$. Pick an e coprime $\phi(n)$. Compute $d \equiv e^{-1} \pmod{\phi(n)}$ using xgcd.

1.6 RSA parameters example

$p = 5, q = 7, n = 5 \cdot 7 = 35, \phi(35) = (5-1)(7-1) = 24$. Pick $e = 5$, $\gcd(5, 24) = 1$. $5^{-1} \equiv 5 \pmod{24}$ so $d = 5$.

Other option $e = 7$ with xgcd:

24	1	0	
7	0	1	quotient 24 div 7 = 3
3	1	−3	7 div 3 = 2
1	−2	7	
r	a	b	

Every row satisfies $r = 24 \cdot a + 7 \cdot b$.

Then $p_k = (5, 35)$, $s_k = 5$ (or $(7, 35), d = 7$).

1.7 Encryption

Message $m < n, m \in \mathbb{N}$.

$$c \equiv m^e \pmod n$$

1.8 Decryption

$$m \equiv c^d \pmod{n}$$

This works because $m' \equiv c^d \equiv m^{e^d} \equiv m^{ed}$ where $ed \equiv 1 \pmod{\phi(n)}$ i.e. $1 + k\phi(n)$ for some k.

$$m' \equiv m^{1+k\phi(n)} \equiv m \cdot 1 \pmod{n}$$

via Lagrange: in $(\mathbb{Z}_{/n})^\times$, $m^{\phi(n)} \equiv 1 \pmod{n}$.

Check that $m^{1+k\phi(n)} \equiv m \pmod{n}$ even when $\gcd(m, n) \neq 1$.

To show this we use the *Chinese Remainder Theorem.*

$m \equiv 0 \pmod{p}, m \equiv a \pmod{q}$, $a \neq 0$.

Then $m^{ed} \equiv 0^{ed} \equiv 0 \pmod{p}$. In $(\mathbb{Z}_{/q})^\times$ we have $a^{q-1} \equiv 1 \pmod{q}$, thus $m^{ed} \equiv a^{1+k\phi(n)} \equiv a^{1+k(q-1)(p-1)} \equiv a \cdot (a^{q-1})^{p-1} \equiv a \cdot (1)^{p-1} \equiv a \pmod{q}$.

So:

$$m^{ed} \equiv 0 \equiv m \pmod{p}$$
$$m^{ed} \equiv a \equiv m \pmod{q}$$

thus the CRT gives $m^{ed} \equiv m \pmod{n}$.

For the case $0^{ed} \equiv 0 \pmod{n}$.

So RSA gives $m' = m$.

1.9 RSA-CRT

For fast encryption, we choose a small e when generating the key.

Choosing small d gives Eve your key, but we can decrypt faster if we use RSA-CRT.

Compute

$$c^d \equiv m_p \pmod{p}$$
$$c^d \equiv m_q \pmod{q}$$

This is faster because the operands are smaller (naively[1] this saves a factor of 4 in each computation, do this twice, so save a factor of 2. Combine m_p and m_q using CRT to get m, this needs just one multiplication given $u = p^{-1} \pmod{q}$, $v = q^{-1} \pmod{p}$. Then $m = m_p \cdot q \cdot v + p \cdot u \cdot m_q$.

2 Lecture 3 Finite Fields

Definition 1. *A set K is a **field** with respect to $\circ$ and $\diamond$, denoted $(K, \circ, \diamond)$ if:*

1. *$(K, \circ)$ is een abelian group.*
2. *$(K^* = K \setminus \{e_\circ\}, \diamond)$ is an abelian group.*
3. *Distributivity holds in K: $a \diamond (b \circ c) = a \diamond b \circ a \diamond c$.*

Definition 2. *A group $(K, \square)$ is **abelian** if these properties hold:*

Closure $\forall a, b \in K$, $a \square b \in K$.

Associativity $\forall a, b \in K$, $(a \square b) \square c = a \square (b \square c)$

Identity $\exists e_\circ \in K$, $\forall a \in K$, $a \square e_0 = a$

[1] "Naively" because Karatsuba double-length multiplication costs only 3 times as much and for very long integers the FFT takes only twice as long

Invertibility $\forall a \in K,\ \exists b \in K,\ a \square b = e_\circ$

Commutativity $\forall a, b \in K,\ a \square b = b \square a.$

Examples of fields and non-fields:
- $(\mathbb{N}, +, \cdot)$ isn't a field: no negative numbers
- $(\mathbb{Z}, +, \cdot)$ isn't a field: no inverse
- $(\mathbb{Q}, +, \cdot)$ is a field

Definition 3. *If $(K, \circ, \diamond)$ and $(L, \circ, \diamond)$ are fields and $K \subseteq L$ then K is a* ***subfield*** *of L.*

Definition 4. *Let L be a field and K be its subfield. The* ***extension degree****, denoted as $[L : K]$ is defined as $\dim_K L$, the dimension of L as a K vectorspace.*

Definition 5. *Let K be a field. The* ***characteristic*** *of K, $\mathrm{char}(K)$ is the smallest positive integer m such that $\underbrace{e_\diamond \circ e_\diamond \circ \cdots \circ e_\diamond}_{m} = e_\circ$. If there is no such m, then $\mathrm{char}(K) = 0$.*

Lemma 1. *The characteristic of a field is either 0 or prime.*

Proof. Let $(K, \circ, \diamond)$ be a field with $\mathrm{char}(K) = n$ and $n > 0$. Assume n isn't prime so $n = a \cdot b$ with $1 < a, b < n$.

Then we have

$$e_\circ = [n]e_\diamond = [a]e_\diamond \diamond [b]e_\diamond. \tag{1}$$

We can show this by

$$\begin{aligned}
&[a]e_\diamond \diamond [b]e_\diamond \\
&= (e_\diamond \circ [a-1]e_\diamond) \diamond [b]e_\diamond \\
&= e_\diamond \diamond [b]e_\diamond \circ [a-1]e_\diamond \diamond [b]e_\diamond \\
&= \cancel{e_\diamond} \diamond [b]e_\diamond \circ [a-1]e_\diamond \diamond [b]e_\diamond && \text{(identity)} \\
&\vdots \\
&= \underbrace{[b]e_\diamond \circ [b]e_\diamond \circ \ldots [b]e_\diamond}_{a \text{ times}} \\
&= [a \cdot b]e_\diamond
\end{aligned}$$

So (1) is true, so either $[a]e_\diamond = e_\circ$ or $[b]e_\diamond = e_\circ$. But by Definition 5 then a or b would be the characteristic of K. So the characteristic can't be the product of two integers.

So any characteristic $n > 0$ must be prime. The characteristic can be 0 by Definition 5. So the characteristic must be either 0 or prime. □

Lemma 2. *A finite field K has $\mathrm{char}(K) \neq 0$, so $\mathrm{char}(K)$ is prime.*

Proof. Since K is finite, there must be $i, j \in \mathbb{N}$ with $[i]e_\diamond = [j]e_\diamond$. Let $i > j$, then $[i - j]e_\diamond = e_\circ$. And so $\mathrm{char}(K) | (i - j)$. □

A field K with $\mathrm{char}(K) = p$ forms a ring inside the field as $e_\diamond, [2]e_\diamond, \ldots, [p-1]e_\diamond, e_\circ, e_\diamond, \ldots$.

A finite field maps to $\mathbb{Z}/p\mathbb{Z}$ as $[i]e_\diamond \mapsto i + p\mathbb{Z}$ or $[i]e_\diamond \mapsto i \mod p$.

Definition 6. *A* ***primefield*** *is the smallest subfield contained in a field K.*

Lemma 3. *Let K be a finite field of $\mathrm{char}(K) = p$. Then there is a primefield of K that is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

$$e_\circ \mapsto 0 \text{ in } \mathbb{Z}/p\mathbb{Z}$$
$$e_\diamond \mapsto 1 \text{ in } \mathbb{Z}/p\mathbb{Z}$$

The vectorspace as linearly independant vectors $\alpha_1, \alpha_2, \ldots, \alpha_n$ with n the dimension. Every element in the field can be written as

$$\sum_{i=1}^{n} c_i \alpha_i \text{ with } c_i \in \mathbb{Z}/p\mathbb{Z}.$$

Lemma 4. *Let K be a finite field. There exists a prime p and an integer $n \in \mathbb{N}_{>0}$ such that $|K| = p^n$ and $\mathrm{char}(K) = p$. (*Notation: $\mathbb{F}_{p^n}$ *or* $\mathrm{GF}(p^n)$*.)*

$$\left(\sum_{i=1}^{n} c_i \alpha_i\right) + \left(\sum_{i=1}^{n} d_i \alpha_i\right) = \sum_{i=1}^{n} (c_i + d_i)\alpha_i$$

so $+ \to \circ$ and $\cdot \to \diamond$.

Lemma 5. *Let K be a finite field. The multiplicative group K^* is cyclic.*
Thus, for every $a \in K^*$ we have $a^{p^n-1} = 1$.

Proof.

$$a^{p^n} = a \Leftrightarrow a \cdot a^{p^n-1} = 1 \cdot a \Leftrightarrow a^{p^n-1} = 1$$

□

Definition 7. ***Polynomial ring over field*** *K*

$$K[x] = \left\{ \sum_{i=1}^{n} a_i x^i | n \in \mathbb{N}, a_i \in K \right\}$$
$$f \in K[x]$$
$$f = \sum f_i x^i$$

Definition 8. *A polynomial $f \in K[x]$ is called* ***irreducible*** *if $\deg(f) \geq 1$ and it cannot be written as the product of polynomials with a smaller degree.*

Some examples

$x^2 - 1 = (x-1)(x+1)$	reducible in $\mathbb{R}[x]$
$x^2 + 1$	irreducible in $\mathbb{R}[x]$
$x^2 + 1 = (x-i)(x+i)$	reducible in $\mathbb{C}[x]$

3 Lecture 4: finite fields continued

An example of GF(4) with symbols can be found in Table 1.

$+$	□	○	⋆	△
□	□	○	⋆	△
○	○	□	△	⋆
⋆	⋆	△	□	○
△	△	⋆	○	□

$\cdot$	○	⋆	△
○	○	⋆	△
⋆	⋆	△	○
△	△	○	⋆

Table 1: An example of GF(4) with addition and multiplication

$\mathrm{GF}(4) = \mathrm{GF}(2^2) = \mathrm{GF}(2)^2$

$$\mathrm{GF}(4) = \left(\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \right\}, +, \cdot \right).$$

Basis:

$$\alpha_1 = \begin{pmatrix}0\\1\end{pmatrix} \qquad \alpha_2 = \begin{pmatrix}1\\0\end{pmatrix}$$

$$\begin{pmatrix}0\\0\end{pmatrix} = 0\cdot\alpha_1 + 0\cdot\alpha_2 = 0 \qquad \begin{pmatrix}1\\0\end{pmatrix} = 0\cdot\alpha_1 + 1\cdot\alpha_2 = \alpha_2$$
$$\begin{pmatrix}0\\1\end{pmatrix} = 1\cdot\alpha_1 + 0\cdot\alpha_2 = \alpha_1 \qquad \begin{pmatrix}1\\1\end{pmatrix} = 1\cdot\alpha_1 + 1\cdot\alpha_2 = \alpha_1 + \alpha_2$$

We can instead use basis $1, a$.

$$0\cdot a + 0\cdot 1 = 0 \qquad 1\cdot a + 0\cdot 1 = a$$
$$0\cdot a + 1\cdot 1 = 1 \qquad 1\cdot a + 1\cdot 1 = a + 1$$

This base vector representation is nice for addition but does not help for multiplication.

4 Security course

5 Security Goals

Confidentiality Third parties cannot read what A and B are saying.

Integrity Third parties cannot modify the contents of the communication.

Authenticity A and B are certain about each other's identities.

Availability Third parties cannot prevent A and B from communicating.

Non-repudiation Someone cannot deny what they have communicated.

Accountability Reliable log of communication history.

6 Crypto primitives

# Keys	Name	Key names	Notation
0	Hash functions	—	$h(m)$
1	Symmetric Crypto	Shared, secret	$K\{m\}$
2	Asymmetric Crypto (public key crypto)	Public & private keypair	$\{m\}_K$

7 Active Attacks

7.1 Replay attack

Intercepted data is sent again. Countermeasures: nonces, timestamps.

7.2 Reflection attack

Data from one session is reused in another session, to for example make the target do encryption/decryption work.

7.3 Man-in-the-middle attacks

Also passive: relay attack. Active involves reencryption. countermeasure: strong authentication.

8 Cipher modes

8.1 Electronic Code Book (ECB)

$m = m_0 m_1 m_2 \cdots \to C = K\{m_0\}, K\{m_1\}, K\{m_2\} \cdots$.

Attack vectors: occurrence frequency, swappping can go unnoticed easily.

8.2 Cipher Block Chaining (CBC)

$$c_0 = K\{m_0 \oplus IV\}$$
$$c_{n+1} = K\{m_{n+1} \oplus c_n\}$$

IV may be sent openly or be constant.

One garbled block means two blocks are lost in deciphering. Last block can be used to verify integrity.

8.3 Output Feedback Mode (OFB)

First, pick a random number (Initialisation Vector, IV) and use it to create a keystream:

$$K\{IV\}, K\{K\{IV\}\}, K\{K\{K\{IV\}\}\} \cdots$$

Then XOR with incoming bitstream. Garbled bits are lost, but only those bits. If sender/receiver are out of sync, everything is lost.

Variation: $c_n = m_n \oplus K\{IV + n\}$ (Counter mode).

8.4 Cipher Feedback (CFB)

$$c_0 = IV$$
$$c_{n+1} = K\{c_n\} \oplus m_{n+1}$$

9 Symmetric Crypto

9.1 Basic Techniques

1. **Substitution**: Swapping characters from the alphabet. Key K is the subsitution function.
2. **Transposition**: Changing positions of characters (by block). K is the position exchange function.
3. **One-time pad**: Take bitwise XOR of message with keystream. K is keystream of at least the same length as the message.

One-time pads are sometimes generated using linear feedback shift registers. See slide 25.

A downside of symmetric crypto is that one needs $\binom{N}{2} = \frac{N(N-1)}{2}$ keys if N people want to communicate pairwise securely.

Also, if key K is lost by A, B is also affected.

9.2 Basic Protocols

9.2.1 Integrity

$$A \longrightarrow B : m, K_{AB}\{h(m)\}$$

Hash function for efficiency.

B can verify integity by decrypting and comparing $h(m)$ with the hash he creates from m.

9.2.2 Confidentiality

$$A \longrightarrow B : K_{AB}\{m\}$$

Only those with K_{AB} can read this, obviously.

When combined with integrity ($A \longrightarrow B : K\{m, K\{h(m)\}\}$) it is important to use different keys, because otherwise if K is compromised, both integrity and confidentiality are broken.

9.2.3 Authenticity

"Shared Secret": You can be authenticated by something only you and the other party know. Problem: secret used in the clear.

It is better to send riddles that can only be solved efficiently using the secret key. The riddle needs to be fresh every time (against replay attacks). Often achieved by using *nonces*.

$$\begin{aligned} A &\longrightarrow B : A, N_A \\ B &\longrightarrow A : K_{AB}\{N_A, N_B\} \\ A &\longrightarrow B : N_B \end{aligned}$$

10 Hashing

10.1 Properties

Preimage Resistant (one-way) Given hash value x, it should be hard to find m with $h(m) = x$.

Second preimage resistant Given an m, it should be hard to find $m' \neq m$ with $h(m) = h(m')$.

Collision resistant It should be hard to find *any* pair $m \neq m'$ with $h(m) = h(m')$.

10.2 Non-revealing commitment

e.g. for flipping coins one can use:

$$\begin{aligned} A &\longrightarrow B : h(C_A, N_A) \\ B &\longrightarrow A : h(C_B, N_B) \\ A &\longrightarrow B : C_A, N_A \\ B &\longrightarrow A : C_B, N_B \end{aligned}$$

(nonces are used to prevent cheating by lookup table - coin outcomes are very limited)

10.2.1 Lamport's hash

C has for each user A a pair $[n \in \mathbb{N}, h^n(\text{passwd}_A)]$.

$$\begin{aligned} A &\to C : A \\ C &\to A : n \\ A &\to C : h^{n-1}(\text{passwd}_A) = x \end{aligned}$$

C can then verify the authenticity of A by checking $h(x) = h^n(\text{passwd}_A)$. C can also then set a new pair $[n-1, x]$ or $[n+1, h(h(x))]$.

11 Asymmetric Crypto

Using two keys: one for decryption (private key, K_d) and one for encryption (public key, K_e).

- Encryption: $\{m\}_{K_e}$
- Decryption: $[c]_{K_d}$.

Identity function:

$$[\{m\}_{K_e}]_{K_d} = m$$

Though for some systems $\{[m]_{K_d}\}_{K_e} = m$ is also valid, this is not a requirement.

12 Number theory

12.1 Equivalence classes

$$\forall N \in \mathbb{N}, n \in \mathbb{Z}, m \in \mathbb{Z}\,[n \equiv m \pmod N \Leftrightarrow \text{ there is a } k \in \mathbb{Z} \text{ with } n = m + k \cdot N]$$

$\mathbb{Z}_N$ is the set of numbers modulo N. Thus

$$\mathbb{Z}_N = \{0, 1, \ldots N-1\}$$

For every $m \in \mathbb{Z}$ we have $m \mod N \in \mathbb{Z}_N$.

If a product modulo N is 1, for instance, $4 \cdot 4 \equiv 1 \pmod{15}$, you can say $\frac{1}{4} = 4 \pmod{15}$. For $\mathbb{Z}_p$ where p is prime, every non-zero number $n \in \mathbb{Z}_p$ has an inverse $\frac{1}{n} \in \mathbb{Z}_p$.

A finite cyclic group often has a generator g that $g^n = k$ so that k can become any number in the group.

12.2 Greatest Common Divisor

$\gcd(n, m)$ = greatest k which divides both n and m. If $\gcd(n, m) = 1$, one calls n, m relative prime.

$$\gcd(n, m) = \begin{cases} \gcd(m, n) & m > n \\ n & m = 0 \\ \gcd(m, n \bmod m) & \text{otherwise} \end{cases}$$

12.3 Extended GCD

$$\text{xgcd}(n, m) = \begin{cases} \text{xgcd}(m, n) & m > n \\ \langle 1, 0 \rangle & n \mod m = 0 \\ \langle y, x - (y \cdot (n \operatorname{div} m)) \rangle & \langle x, y \rangle = \text{xgcd}(m, n \mod m) \end{cases}$$

Results in the solutions a, b for $a \cdot m + b \cdot n = \gcd(m, n)$.

13 RSA

RSA has a public key e, a private key d and a modulo $n = p \cdot q$.
Public key: (n, e)
Private key: (n, d)

13.1 RSA key creation

1. Pick two primes p and q. $n = pq$
2. Calculate $\phi(n) = (p-1)(q-1)$.
3. Pick e from $\mathbb{Z}^*_{\phi(n)}$.
4. Calculate d from $\frac{1}{e} \in \mathbb{Z}^*_{\phi(n)}$ using xgcd$(\phi(n), e)$.

13.2 Encryption / Decryption

Encrypt using RSA by $c = m^e \mod n$
Decrypt using $m = c^d \mod n$.

13.3 Signatures with RSA

$$A \longrightarrow B : m, [h(m)]_{d_A}$$

Works because RSA is symmetric and since only A has access to d, only he can have encrypted it.

13.3.1 Blind signatures

1. A computes $m' = r^e \cdot m \mod n$, where r is a random number, and gives this to B.
2. B signs m', giving $k = [m']^d \mod n$ to A.
3. A computes $\frac{k}{r} = \frac{r^{ed} \cdot m^d}{r} = \frac{r \cdot m^d}{r} = m^d \mod n$

Can be used for anonymous signatures on e-cash, e-voting...

13.4 Certificates

A certificate is a public key that has been signed by a thrusted third party.

14 Diffie-Hellman Key Exchange

Using a generator g in a finite cyclic group:

$$A \longrightarrow B : A, g^{s_A}$$
$$B \longrightarrow A : B, g^{s_B}$$

Then $K_{AB} = g^{s_A s_B} = (g^{s_A})^{s_B} = (g^{s_A})^{s_B}$.
This is not authentication!

15 El-Gamal

Fix a generator $g \in G$ of size N.
Private key: $n \in \mathbb{N}$ with $n < N$.
Public key: $h = g^n \in G$.

15.1 Encryption / Decryption

15.1.1 Encryption

1. Represent message as $m \in G$.
2. Choose a random $r < N$.
3. $\{m\}_h = (g^r, m \cdot h^r)$.

15.1.2 Decryption

1. Ciphertext $c = (c_1, c_2)$ with $c_i \in G$.
2. $$[(c_1, c_2)]_n = \frac{c_2}{(c_1)^n} = \frac{m \cdot h^r}{(g^r)^n} = \frac{m \cdot (g^n)^r}{(g^r)^n} = m$$

15.1.3 Signatures

Choose random $r < p - 1$ in $\mathbb{Z}_p^*$ with $\gcd(r, p-1) = 1$ and then:

$$\text{sign}_n(m) = \left(g^r, \frac{H(m) - n \cdot g^r}{r} \mod p - 1 \right)$$

Verification of signature (s_1, s_2):

$$g^{H(m)} \stackrel{??}{=} s_1^{s_2} \cdot h^{s_1}$$