



# Network Security

## Summary

Author: Thomas Pettinger

**2017-03-02**

Network Security  
TECHNISCHE UNIVERSITÄT MÜNCHEN

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Attacks and Attack Detection . . . . .	1
1.2	Attacker Model and Locations . . . . .	1
1.3	Security Goals . . . . .	1
1.4	Threads . . . . .	2
<b>2</b>	<b>Language-theoretic Security</b>	<b>3</b>
<b>3</b>	<b>Firewalls and Security Policies</b>	<b>4</b>
3.1	The three Security Components . . . . .	4
3.2	Network Firewalls . . . . .	4
<b>4</b>	<b>TCP SYN Cookies</b>	<b>8</b>
4.1	TCP SYN Flood Attack . . . . .	8
4.2	TCP SYN Cookies . . . . .	8
<b>5</b>	<b>Cryptography</b>	<b>9</b>
5.1	Security of Cryptographic Schemes . . . . .	9
5.2	Symmetric Cryptography . . . . .	9
5.3	Hash Functions . . . . .	15
5.4	Asymmetric Cryptography . . . . .	16
5.5	Hybrid Approach . . . . .	18

---

# 1 Introduction

## 1.1 Attacks and Attack Detection

Attacks can have different impacts on the target. Disruptive attacks try to fully deny the service (DoS) of the victim whereas degrading ones only occupy parts of the resources. A DoS attack can also be executed distributed, a so called DDoS. Attackers might also try to gain confidential data or control the target system. Port scans can be used to gain information about the network topology, operating systems and applications or application versions.

To be able to tell if a system is under attack, different measures can be taken at different points in the system.

Host intrusion detection systems (HIDS) are located on the host system. This enables easy detection using information available on the potential victim system but it has to be present on every system (expensive deployment) and the attack actually reaches the victim and is not detected in advance. Network intrusion detection systems (NIDS) lay on the network layer which enables the detection of attacks before they reach the host.

One of the detection methods available is knowledge-based detection. Known signatures of attacks are compared to the actual traffic and if the patterns match an alarm is raised. This only detects known attacks though. To improve this shortcoming, anomaly detection in traffic, protocol or application behavior can be used. Anomalies can be detected with different metrics in mind. A very simple one might be the number of requests, but this does not take legitimate change in traffic into account. A better approach is using cumulative sums which are low if the average is small or whenever only small amounts of values are large but grows if the amount of large values grows in a certain point in time. The disadvantage of anomaly detection though is that oftentimes the rate of false-positives is high.

Detecting attacks is not easy and network monitoring often comes at a cost. It is important though especially in large systems when the attack surface grows. The challenge is to find a good compromise between security and performance.

## 1.2 Attacker Model and Locations

We generally assume the attacker to be (in) the network. They can perform any active or passive attack but cannot break cryptographic primitives. Active attacks are attacks where some influence is measurable e.g. a delay, modifications or replays whereas a passive attack simply stands for eavesdropping messages. This model is called the Dolev-Yao attacker model.

Attackers can be located on different parts of the network and depending on this location different attacks are possible. If the attacker is close to you they are able to perform active attacks like message modifications on you. This can be circumvented by communicating over a secure tunnel though. If the attacker is close to your servers, timing attacks are possible where attackers can measure how long certain operations take to break into the system. The last possibility is that the attacker is somewhere in the Internet. Since the end user has no control over how packets are routed, attackers can modify the path they take for example.

## 1.3 Security Goals

**Data Integrity** No improper or unauthorized change of data

**Confidentiality** Concealment of information

**Availability** Services should be available and function correctly

---

**Authenticity** Entity is who she claims to be

**Accountability** Identify the entity responsible for any communication event

**Controlled Access** Only authorized entities can access certain services or information

## 1.4 Threads

We define a thread in a communication as any possible event or sequence of actions that might lead to a violation of one or more security goals. The actual realization of a thread is then called attack.

Different threads are possible:

- **Masquerade:** An entity claims to be another entity (also called “impersonation”)
- **Eavesdropping:** An entity reads information it is not intended to read
- **Loss or Modification of (transmitted) Information:** Data is being altered or destroyed
- **Denial of Communication Acts (Repudiation):** An entity falsely denies its participation in a communication act
- **Forgery of Information:** An entity creates new information in the name of another entity
- **Sabotage/Denial of Service:** Any action that aims to reduce the availability and / or correct functioning of services or systems
- **Authorization Violation::** An entity uses a service or resources it is not intended to use

---

## 2 Language-theoretic Security

Communication protocols define the procedure and the format of exchanged messages. If two communication partners speak the same protocol it is not necessarily given that they have the same understanding though. Different problems may arise which result in some guidelines to avoid them:

**Full input recognition** Programmers usually assume well formed input where in reality the input is controlled by the attacker. For this reason every input should be checked if it fulfills the expectations of valid inputs.

**Only Type 2 or 3 of Chomsky Hierarchy grammars for inputs** Do not define turing-complete protocols because recognition of the input and testing the equivalence of implementations is undecidable.

Grammar	Language	Recognized by
Type 3	Regular	Finite state automaton
Type 2	Context-free	Pushdown automaton
Type 1	Context-sensitive	Some weird stuff
Type 0	recursively enumerable	Turing machine

Figure 1: Chomsky Hierarchy of Languages

**Reduce computing power** Reduce the computing power exposed to the outside. Computing power that is not there can not be exploited. This also includes defining protocols only in type 2 or 3 languages since parsing types 0 and 1 requires large or potentially unlimited amounts of computing.

**Same interpretation of messages** All participants of a communication should interpret messages the same way. For this parsers have to be equivalent which is only decidable for type 2 and 3.

---

## 3 Firewalls and Security Policies

We define a system as secure if, started in an allowed state, always stays in states that are allowed.

### 3.1 The three Security Components

- **Requirements** define security goals
- **Policy** are rules to implement the requirements
- **Mechanisms** enforce the policy

### 3.2 Network Firewalls

Firewalls provide **controlled access** at the network level to resources. They are usually deployed where a protected subnet is connected to a less trusted network like the internet (c.f. Figure 2). From the firewall's point of view, there are incoming and outgoing packages on all interfaces. These can be filtered using two different strategies.

**Whitelisting**, which is considered as the best practice, has the default behavior of denying all packets and allowing only explicitly permitted ones whereas **blacklisting** allows everything except blocked packets.

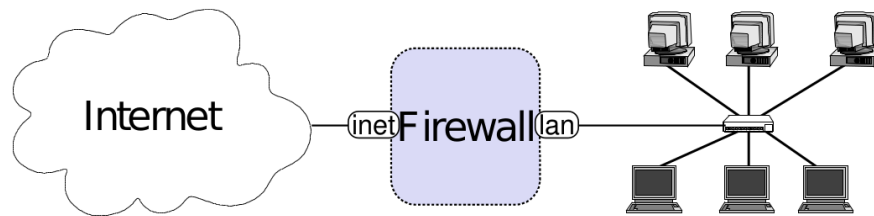


Figure 2: Firewall Placement

#### Configuring Firewalls

Firewalls are configured with rulesets which are traversed sequentially until a matching one is found. Those rules are composed of a matching condition and an action. Possible actions are for example accept, drop, reject or log. The matching conditions are a bit more complex. They include the incoming interface, several layer 2 to 4 packet fields (srcMAC, dstMAC, srcIP, dstIP, prot, srcPort, dstPort, flags,...), states (in case of stateful matching) and other relevant conditions.

#### Stateful Firewalls

Stateful Firewalls keep states of connections with the help of IP-5-Tuples (srcIP, dstIP, protocol, srcPort, dstPort). A new state is generated when a packet with a new tuple arrives which transitions from NEW to ESTABLISHED state. It is usually advisable to put more frequently used rules to the top of the firewall, i.e. matching established connections (new connections are rarer) and to check that ports are above the well defined port range ( $\geq 1024$ ). Figure 3 shows an example of a stateful firewall configuration.

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	> 1023	80	New	Accept
C	lan	internal	external	TCP	> 1023	80	New	Accept
D	lan	internal	external	UDP	> 1023	53	New	Accept
E	*	*	*	*	*	*	*	Drop

Figure 3: Stateful Firewall Configuration

## Stateless Firewalls

Stateless firewalls do not generate states for incoming connections but only operate on single packets since keeping states is expensive and needs fast memory. For this reason lookup times are in  $\mathcal{O}(\#rules)$  which, for large  $\#rules$  is slower than stateful filtering ( $\mathcal{O}(1)$ ). For small  $\#rules$  stateless filtering is faster though due to the lack of memory writes. It is also more complex to configure which makes the approach more error prone. An example for a stateless ruleset is shown in Figure 4.

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B <sub>1</sub>	inet	external	webserver	TCP	> 1023	80	*	Accept
B <sub>2</sub>	lan	webserver	external	TCP	80	> 1023	Yes	Accept
C <sub>1</sub>	lan	internal	external	TCP	> 1023	80	*	Accept
C <sub>2</sub>	inet	external	internal	TCP	80	> 1023	Yes	Accept
D <sub>1</sub>	lan	internal	external	UDP	> 1023	53	-	Accept
D <sub>2</sub>	inet	external	internal	UDP	53	> 1023	-	Accept
E	*	*	*	*	*	*	*	Drop

Figure 4: Stateless Firewall Configuration

Stateless firewalls usually look at the ACK flag of TCP connection to determine approximately if connections are new or established. When a SYN/ACK packet is sent as first packet of a connection, the firewall will pass it but the host will drop it if implement properly.

## Spoofing Protection

Spoofing is the forgery of IP addresses by filling the source IP field with another IP than one's own. Spoofing protection then allows only IP addresses that belong to you on outgoing connections. For incoming traffic this is more difficult since we can not determine where the packet actually came from so we are only able to block our and special purpose IPs.

## Common Errors

- How is your firewall management interface reachable?
- What is allowed over the Internet?
- IPv4 and IPv6?
- Outbound rule ANY? (c.f. spoofing)
- Policy's vs. Firewalls understanding of Inbound and Outbound?
- Shadowing: unreachable firewall rules

---

## What Firewalls cannot do

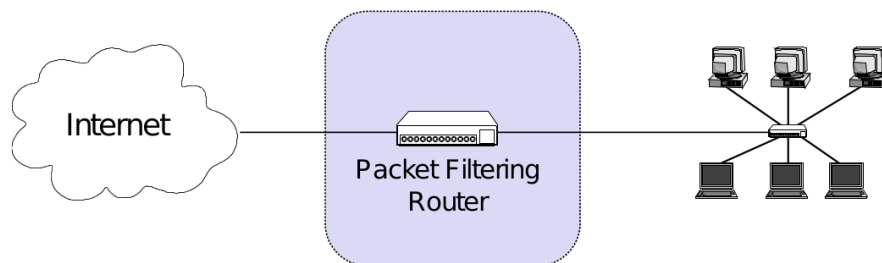
- can't protect against malicious insiders
- can't protect against connections that don't go through it
- can't protect against completely new threats
- can't fully protect against viruses
- does not perform cryptographic operations, e.g. message authentication
- can't set itself up correctly

## Bastion Hosts

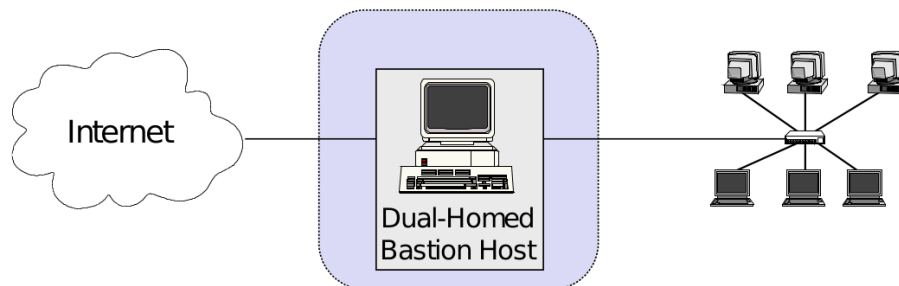
A bastion host is a host that is more exposed to the hosts of an external network than the other hosts of the network it protects. When configuring, one should keep in mind that it might get compromised so do things like disabling SSH password login, do not allow it to sniff internal traffic or disable user accounts.

## Firewall Architectures

**Simple Packet Filter Architecture** Packet filtering is done through a filtering router or firewall with two interfaces.

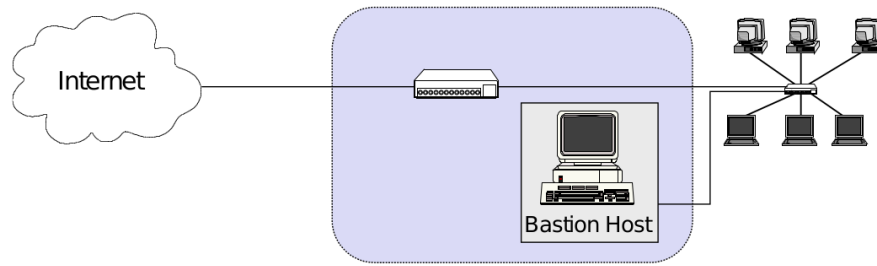


**Dual-Homed Host Architecture** The bastion host is part of two networks and is firewall and application proxy. Disadvantage: bastion host is bottleneck

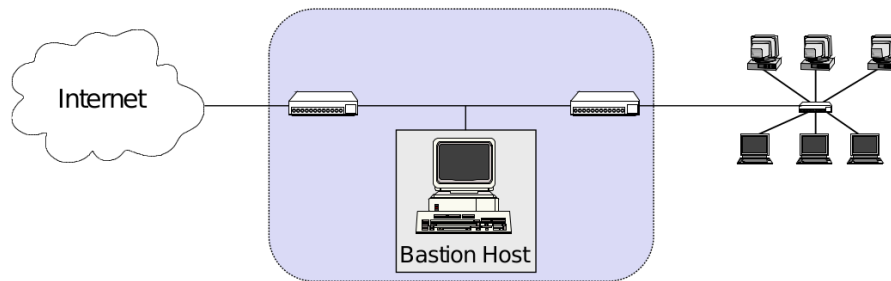


**Screened Host Architecture** The bastion host is proxy, located in the internal network and thus protected by the firewall.





**Screened Subnet Architecture - DMZ** A demilitarized zone (DMZ) is configured hosting the bastion host (proxy) and publicly accessible servers. The second packet filter is an additional protection measurement in case the DMZ gets compromised.



---

## 4 TCP SYN Cookies

### 4.1 TCP SYN Flood Attack

During an TCP SYN Flood Attack an attacker sends large amounts of packets with spoofed source addresses to the victim. This fills up their connection table with half open connections (sequence numbers) which results in legitimate users not being able to establish new TCP connections. A solution for this are TCP SYN cookies.

### 4.2 TCP SYN Cookies

TCP SYN Cookies are particularly chosen initial sequence numbers  $\alpha = h(S, K_{SYN})$  where  $K$  is a secret key,  $S_{SYN}$  the source address of the SYN packet and  $h$  a cryptographic hash function. On arrival of the ACK message, Bob calculates  $\alpha$  again and checks if the ACK number is correct ( $\alpha + 1$ ). This process is shown in Figure 5.

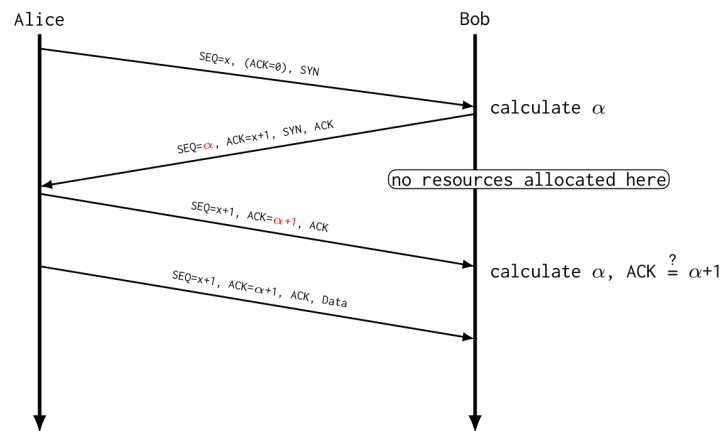


Figure 5: TCP SYN Cookies

#### Pros

- No resource allocation after SYN packets
- Client does not have to be aware of the server using SYN cookies
- No changes in the TCP protocol necessary

#### Cons

- Calculating  $\alpha$  may be CPU consuming (Linux implementation: CPU local with high caching efficiency)
- TCP options (like large windows size) cannot be negotiated (Linux implementation: window size hacked into cookie, SYN cookies only enabled if a threshold of connections is exceeded)
- Efficient implementations might be vulnerable to cryptanalysis (Linux implementation: SHA used, counter updated every minute)

---

## 5 Cryptography

Cryptography is the field of science which is concerned with secure communication. It provides cryptographic schemes to achieve confidentiality (ciphers) and authenticity (message authentication codes).

### 5.1 Security of Cryptographic Schemes

A secure scheme is defined as a scheme, for which it is impossible for a probabilistic polynomial adversary to break it with at most negligible probability. Negligibility is defined as  $f(n) < \frac{1}{p(n)}$  for a polynomial  $p$  and sufficiently large  $n$ , e.g.  $f(n) = \frac{1}{2^n}$ .

Kerckhoff's principle states that the cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience. Thus only the key needs to be secret.

It is advisable to use only standardized schemes from libraries and RTFM (read the fucking manual) because implementing own schemes has a lot of pitfalls and is more often or almost always done wrong. One also has to keep in mind, that encryption alone does not imply that the system is secure, often integrity and authenticity are more important than confidentiality. And also do not forget key management.

#### Security of Ciphers

We define a cipher as secure if it is impossible for attackers to recover the key, the entire or even any character of the plaintext from the ciphertext. This is the case if it is indistinguishable from a random string with uniform distribution of the character probabilities.

### 5.2 Symmetric Cryptography

In symmetric encryption two communication partners Alice and Bob share a secret key that is used for encryption and decryption or message authentication.

We use the following terminology:

- $\leftarrow$  non-deterministic assignment
- $:=$  deterministic assignment
- Key  $k \leftarrow \text{Gen}(1^n)$
- Plaintext  $m = \text{Dec}_k(c)$
- Ciphertext  $c = \text{Enc}_k(m)$
- $\text{Dec}_k(\text{Enc}_k(m)) = m$

#### 5.2.1 One-Time-Pad (OTP): A Perfect Cypher

For the OTP a perfectly random bitstream  $otp$  with the length of the message to encode is needed. Then the encryption operation is defined as  $\text{Enc}_{otp}(m) = m \oplus otp$  and the decryption operation as  $\text{Dec}_{otp}(c) = c \oplus otp$ . For the OTP to be perfectly secure, the key must only be used once which is impractical in the real world where we usually want  $\text{length}(k) \ll \text{length}(m)$  and thus reusable keys.

#### 5.2.2 Attacking Symmetric Ciphers

The goals of attacks on ciphers is to learn something about  $m$  given a  $c$ . Getting any information about  $k$  from an attack is also considered a successful one.

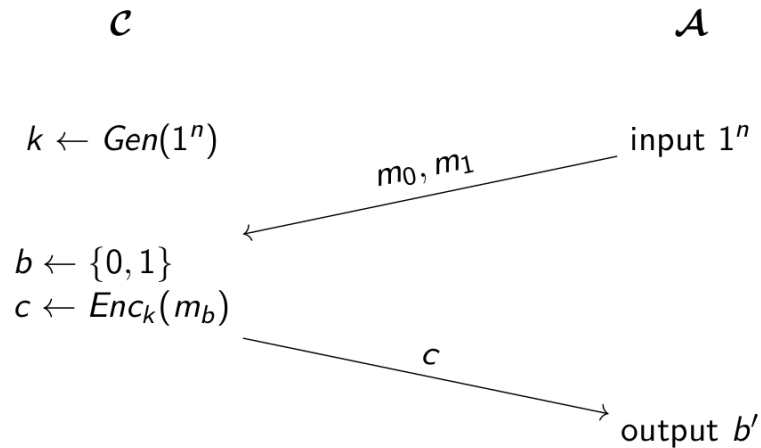
To analyze the security, cryptography uses attack games where  $\mathcal{C}$  is the challenger and  $\mathcal{A}$  the adversary. Possible attack scenarios are listed in the following, of which some are explained more precisely below:

- Ciphertext-only-attack: attacker knows  $c$

- 
- Known-plaintext-attack: For a fixed  $k$ , the attacker got a pair  $(m, c)$  and tries to learn something about other ciphertexts
  - Chosen-plaintext (CPA) and chosen-ciphertext attack: similar to previous attack, but attacker can chose  $m$  or  $c$  freely

We consider symmetric ciphers to be secure if they withstand CPA.

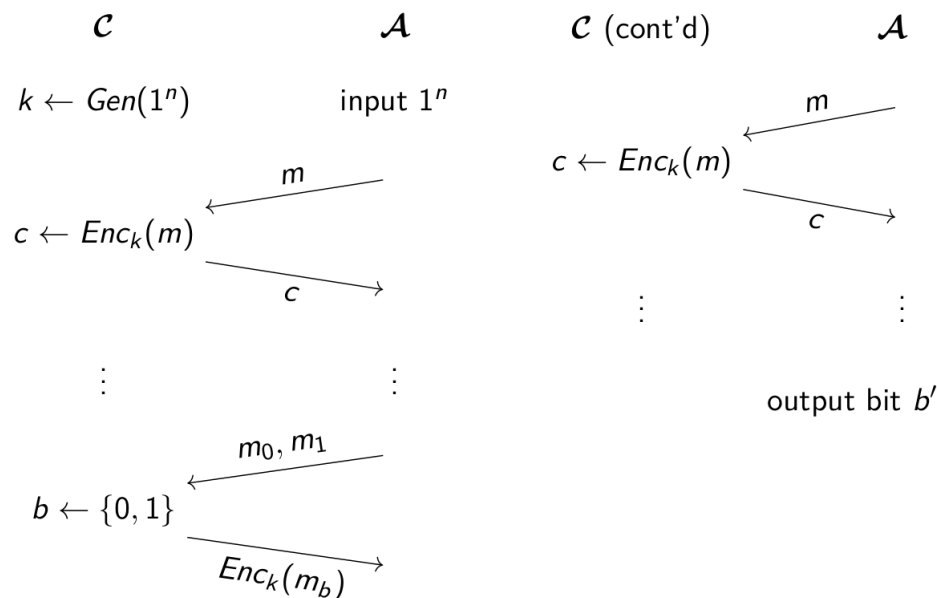
### The Eavesdropping Experiment



In the eavesdropping experiment,  $\mathcal{C}$  first generates a random key  $k$ . After that,  $\mathcal{A}$  sends them two messages  $m_0$  and  $m_1$  for encryption with  $|m_0| = |m_1|$ .  $\mathcal{C}$  then chooses one of the two messages and encrypts it. If  $\mathcal{A}$  can tell which message  $\mathcal{C}$  chose, the attack was successful. If this happens with probability  $0.5 + \text{negligible}$  the used cipher is secure.

---

## Chosen-plaintext Attack



In the chosen-plaintext attack the first step again is that  $\mathcal{C}$  generates a random key  $k$ .  $\mathcal{A}$  is then allowed to send an arbitrary amount of messages to  $\mathcal{C}$  who will encrypt and send them back to  $\mathcal{A}$  which means that  $\mathcal{C}$  is an “oracle” for  $\mathcal{A}$ . At some point,  $\mathcal{A}$  will send two messages  $m_0$  and  $m_1$  of equal length of which  $\mathcal{C}$  chooses one, encrypts it and sends the result back to  $\mathcal{A}$ .  $\mathcal{A}$  is then again allowed to use  $\mathcal{C}$  as oracle for an arbitrary amount of messages and if they are at some point able to tell which message ( $m_0$  or  $m_1$ )  $\mathcal{C}$  encrypted, the attack is successful.

### 5.2.3 Block and Stream Ciphers

A block cipher encrypts and decrypts inputs of length  $n$  to outputs of length  $n$  ( $\Rightarrow$  block length  $n$ ). A stream cipher on the other hand generates a random bitstream with arbitrary length, called keystream, that is xored to the plain text to encrypt and decrypt.

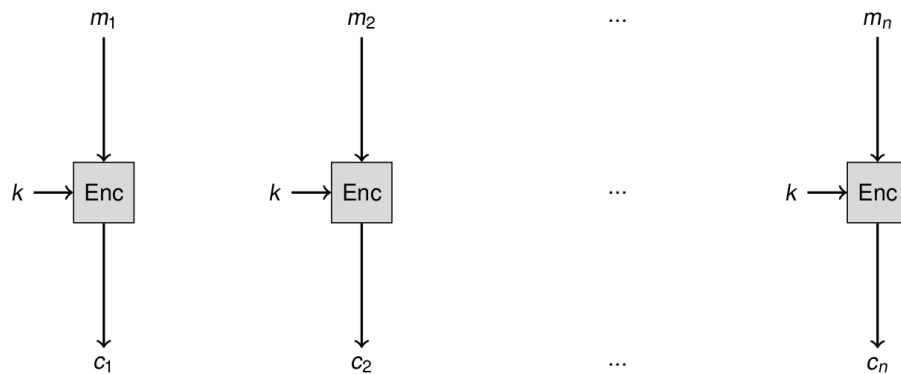
The most advisable cipher to use is probably the AES block cipher. It is well tested and proven to be (mostly) secure and hardware supported what makes it quite fast ( $> 2GB/s$  with HW support,  $200Mbit/s$  without).

### 5.2.4 Modes of Encryption

Modes of encryption are necessary to handle messages of variable length with block ciphers. The plaintext therefore is split into parts of length equal to the cipher block length. If the last block is shorter than the block length, we add padding.

---

### 5.2.5 Electronic Code Book Mode (ECB)



In ECB, every plaintext block is encrypted with the unmodified key as input. The problem thereby is that identical plaintext blocks result in the same ciphertext blocks.



### 5.2.6 Cipher Block Chaining Mode (CBC)

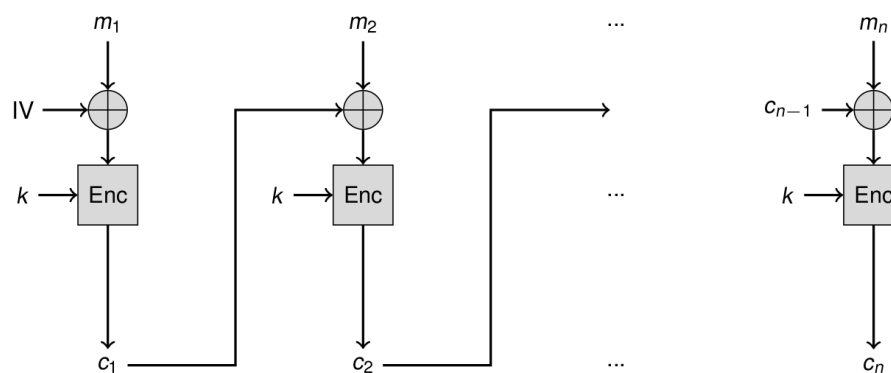


Figure 6: CBC Encrypt

CBC uses the ciphertext from the previous block xored with the current message block and the unmodified key  $k$  as inputs of the encryption function  $c_i = Enc_k(c_{i-1} \oplus m_i)$ . For the first message, where no previous cipher block is available, an initialization vector (IV) is used which may be sent in plaintext and is fresh for every message (or packet if the message is split across multiple packets).

Compared to ECB, the advantage is that equal plaintext blocks/messages are not encrypted to the same ciphertext blocks/messages.

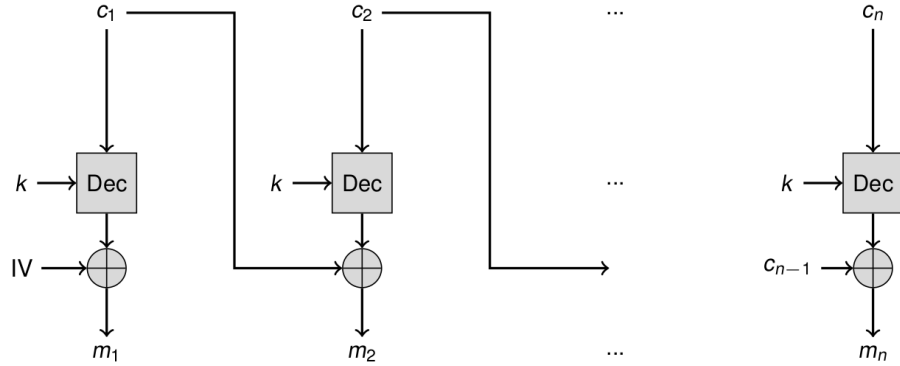


Figure 7: CBC Decrypt

Decryption is defined by  $m_i = c_{i-1} \oplus Dec_k(c_i)$ .

### 5.2.7 Output Feedback Mode (OFB)

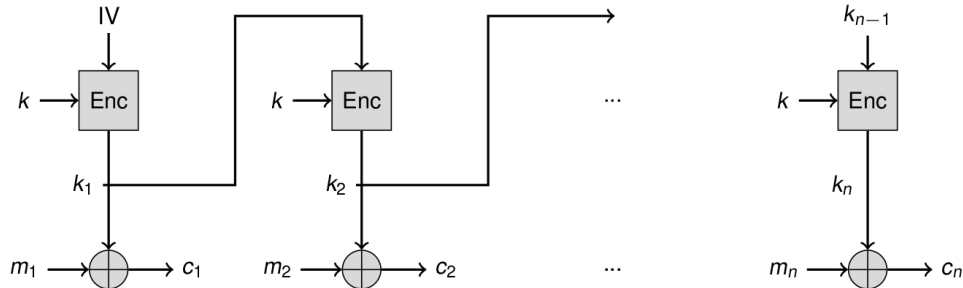


Figure 8: OFB Encrypt

OFB transforms a block cipher into a stream cipher. In step  $i$ , it takes cipher key  $k_{i-1}$  from the previous step and encrypts it with the key  $k$ . This cipher key  $k_i$  is then xored with the corresponding plaintext block  $m_i$  to calculate the ciphertext  $c_i$ . In the first step an IV is used as  $k_{i-1}$ .

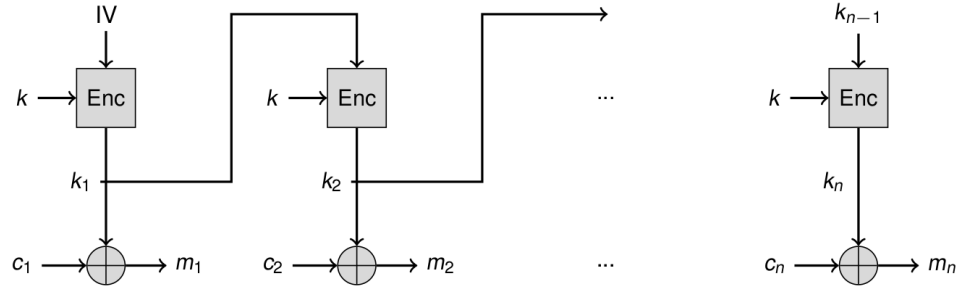


Figure 9: OFB Decrypt

Decryption is the same procedure except that the key stream is xored with the cipher text blocks.

### 5.2.8 Counter Mode (CTR)

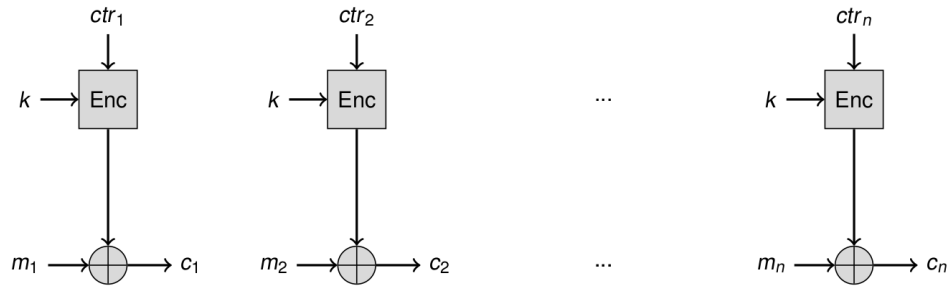


Figure 10: CTR Encrypt

In step  $i$ , CTR encrypts a counter  $ctr_i = IV || i$  with key  $k$  and xors the result with the plaintext block  $m_i$ . Like OFB, CTR also transforms block ciphers into stream ciphers.

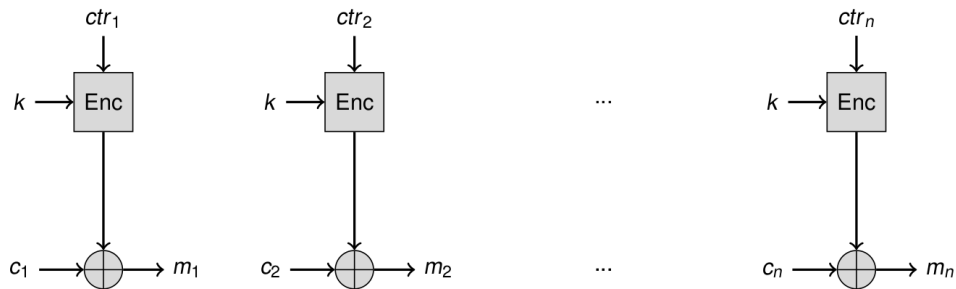


Figure 11: CTR Decrypt

Decryption is done by  $m_i = Enc_k(ctr_i) \oplus c_i$ .



---

### 5.2.9 Message Authentication Code (MAC)

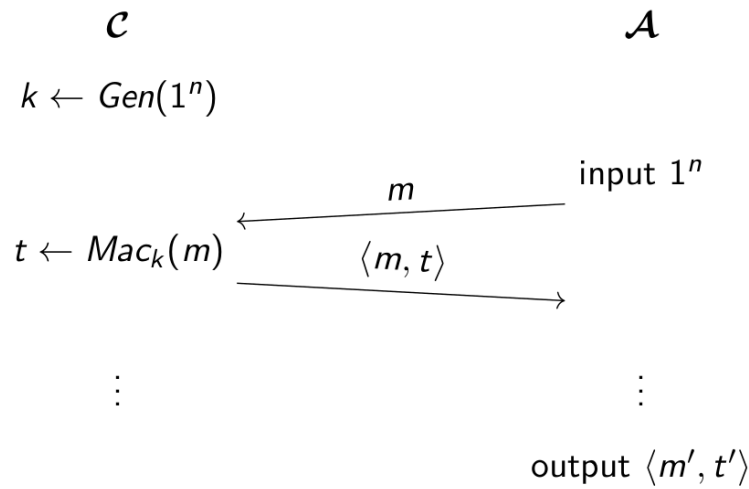
MACs are used in symmetric cryptography to ensure message authenticity but do not provide replay protection. They are transmitted with the message  $\langle m, t \rangle$ . In practice, MACs are either based on hash functions (HMAC), CBC (CMAC) or included in the encryption (authenticated encryption modes).

We define the following terminology:

- Key  $k \leftarrow \text{Gen}(1^n)$
- Tag  $t \leftarrow \text{Mac}_k(m)$
- Verification  $b := \text{Vrfy}_k(m, t)$  where  $b = 1$  means valid and  $b = 0$  invalid

We define a MAC as secure, if it withstands the adaptive chosen-message attack.

#### Adaptive Chosen-message Attack



In the adaptive chosen-message attack  $\mathcal{C}$  first generates a random key  $k$ .  $\mathcal{A}$  then sends an arbitrary amount of messages to  $\mathcal{C}$  for which they answer with a message consisting of the original message and a tag  $t$ . At some point,  $\mathcal{A}$  will generate a message-tag pair  $\langle m', t' \rangle$  where  $m$  was not previously sent to  $\mathcal{C}$ . The attack is successful, iff  $\text{Vrfy}_k(m', t') = 1$ , so if  $\mathcal{A}$  was able to generate a valid MAC tag for a new message.

### 5.2.10 Combining Confidentiality and Authentication

Generally the best approach to combine confidentiality and authentication is to first encrypt and then authenticate, i.e.  $c \leftarrow \text{Enc}_{k_1}(m)$ ,  $t \leftarrow \text{Mac}_{k_2}(c)$  and transmit  $\langle c, t \rangle$ .

## 5.3 Hash Functions

Hash functions are functions which take inputs of arbitrary and transform them to a fixed length output. Cryptographic hash functions must also have the following properties:

- **Pre-image resistance:** It is infeasible to find an  $x'$  s.t.  $H(x') = H(x)$  for given  $H(x)$  and randomly chosen  $x$ .
- **Second pre-image resistance:** It is infeasible to find an  $x' \neq x$  s.t.  $H(x') = H(x)$  for a given  $x$ .
- **Collision resistance:** It is infeasible to find  $x' \neq x$  s.t.  $H(x) = H(x')$ .

## 5.4 Asymmetric Cryptography

In asymmetric cryptography, the two communication partners no longer have one shared key, but each participant has a key pair. A private/secure key ( $sk$ ) that is only known to one person and is used for decryption and message signing and a public key ( $pk$ ) that can be published and is used for encryption and message verification. Asymmetric cryptography is based on mathematical problems which are believed to be hard (e.g. integer factorization). It only needs an authenticated channel to exchange keys of which less amounts are required than in the symmetric setting. It is orders of magnitudes slower though.

### 5.4.1 Public-key Encryption Scheme

1.  $(pk, sk) \leftarrow Gen(1^n)$
2. Encryption with public key:  $c \leftarrow Enc_{pk}(m)$
3. Decryption with private key:  $m := Dec_{sk}(c)$

### RSA

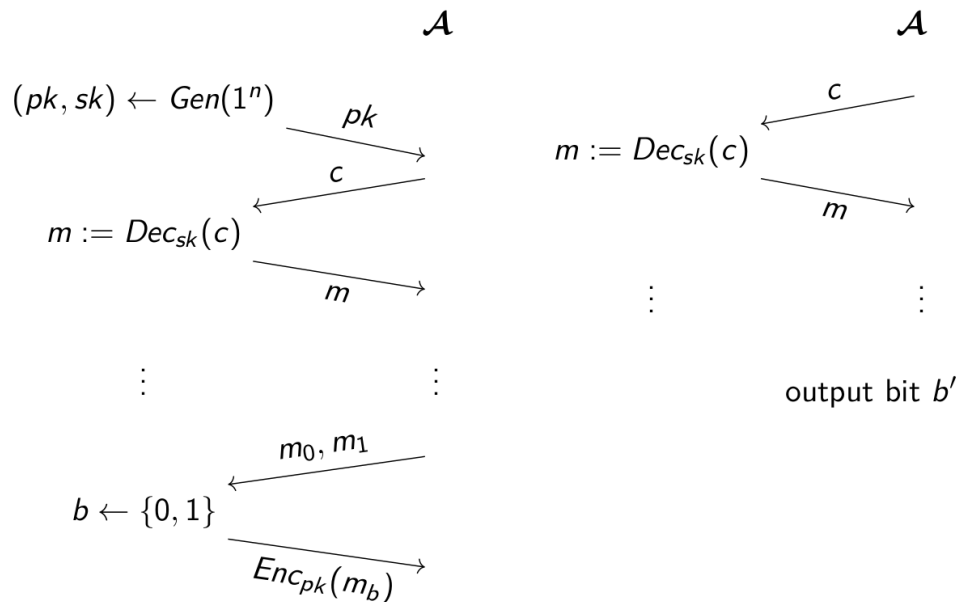
Key generation in RSA is done with the following procedure:

1.  $(N, p, q) \leftarrow GenModulus(1^n)$
2.  $\phi(N) := (p-1)(q-1)$
3. find  $e$ :  $\gcd(e, \phi(N)) = 1$
4.  $d := [e^{-1} \text{ mod } \phi(N)]$
5.  $pk = \langle N, e \rangle$
6.  $sk = \langle N, d \rangle$

Encryption then is defined as  $RSA_{pk}(y) := [y^e \text{ mod } N]$  and decryption as  $RSA_{sk}(y) = [z^d \text{ mod } N]$ .

### Chosen-ciphertext Attack (CCA)

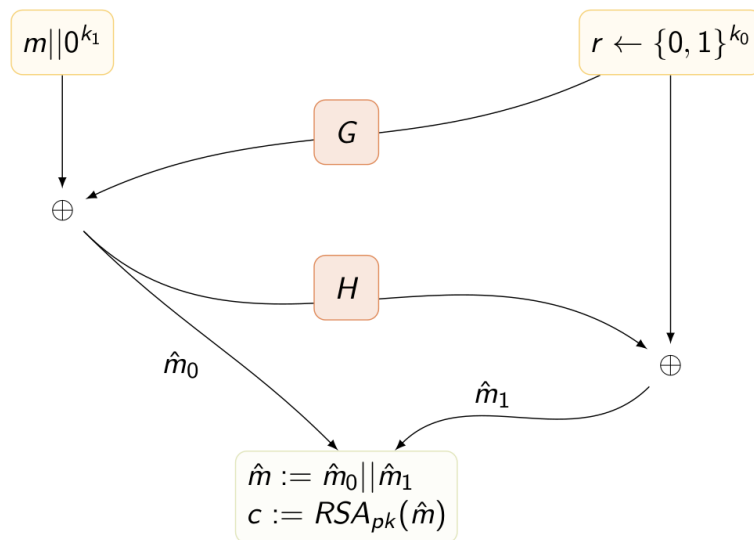
An asymmetric encryption scheme is considered secure if it withstands CCA.



CCA is quite similar to CPA except  $\mathcal{A}$  sends ciphertext messages to  $\mathcal{C}$  for probing instead of plaintext ones. A restriction not depicted in the illustration above is that  $\mathcal{A}$  may not request a decryption for  $Enc_{pk}(m_b)$  itself.

### Optimal Asymmetric Encryption Padding (OAEP)

OAEP is a padding scheme for asymmetric encryption depicted below.



RSA used in conjunction with OAEP is secure under CCA.

### 5.4.2 Signature Scheme

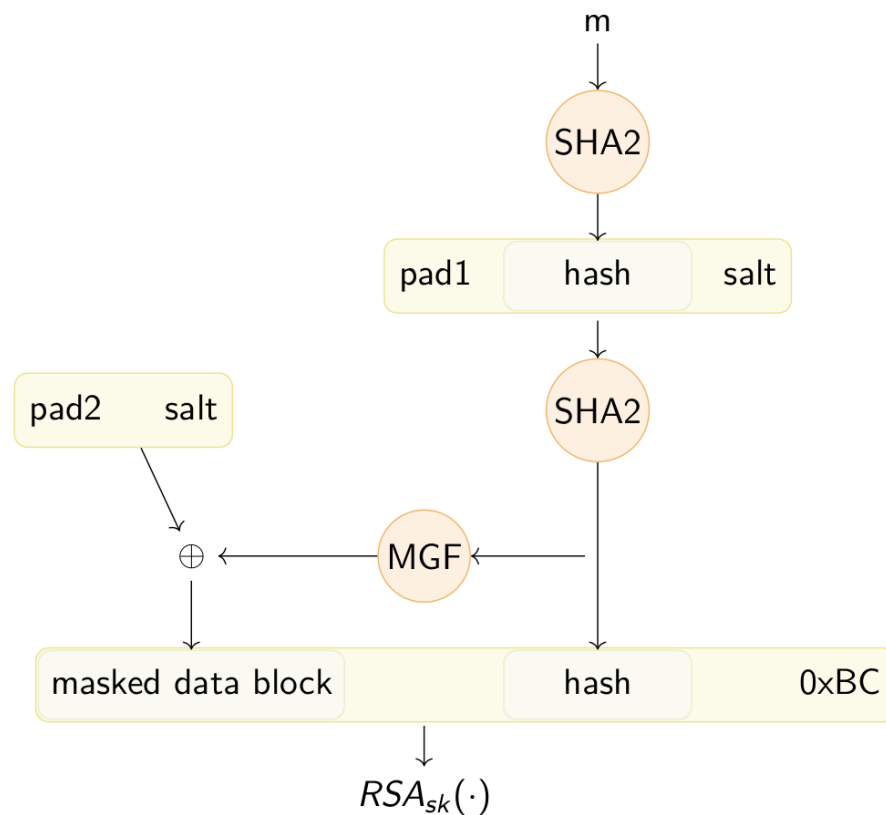
1.  $(pk, sk) \leftarrow Gen(1^n)$
2. Signature generation with private key:  $\sigma \leftarrow Sign_{sk}(m)$
3. Signature verification with public key:  $b := Vrfy_{pk}(m, \sigma)$  where  $b = 1$  means valid and  $b = 0$  invalid

Signatures are often slower than their MAC relatives and provide non-repudiation. A signature scheme is considered secure if it withstands the adaptive chosen-message attack.

---

## RSASSA-PSS

RSASSA-PSS is a signature scheme that uses RSA.



RSASSA-PSS is secure under adaptive chosen-message attack and breaking it would mean that RSA is broken.

## 5.5 Hybrid Approach

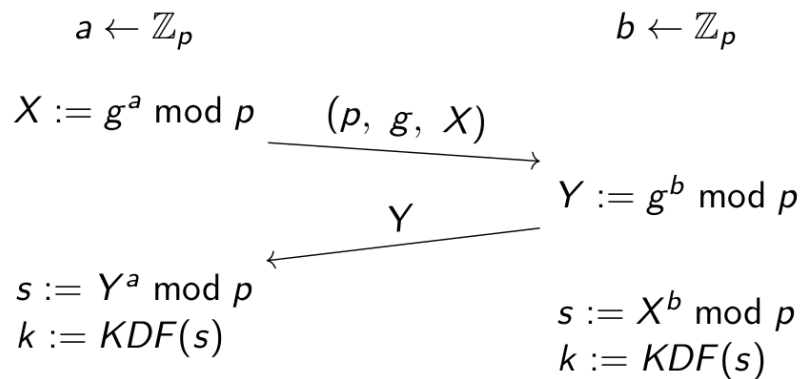
Since public key cryptography is slower than secret key cryptography, a hybrid approach is often advisable. Public-key cryptography is used to protect a shared key (session key) that is used for any further communication via secret-key cryptography. The private key for the key exchange is called long-term key.

**Perfect forward security** is often an important property of this approach. It states that if an attacker gains access to the long-term key or the session key, they should not be able to decrypt messages of past sessions.

A common strategy is to use a signed Diffie-Hellman key exchange and a secret-key authenticated encryption scheme for communication. To guarantee perfect forward secrecy, DH keys have to be calculated for every connection and old keys have to be wiped.

---

### 5.5.1 Diffie-Hellman Key Exchange (DH)



In the first step of the DH key exchange, communication partner A selects a prime  $p$ , a generator  $g$  which is a primitive root for the cyclic group of  $\mathbb{Z}_p$  and a random number  $a \in \mathbb{Z}_p$ . A then calculates  $X = g^a \bmod p$  and sends it with  $p$  and  $g$  to B. B also chooses a random number  $b \in \mathbb{Z}_p$  and calculates  $Y = g^b \bmod p$  which they send back to A. Both can then calculate the key  $k$  by  $k = Y^a = g^{ba} = g^{ab} = X^b \bmod p$ .