Modern Cryptology – Test formulae sheet

Based on a paper written by Guy Shaked in 2011. Translated to English by Dekel Santo in 2014.

DES Encryption

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \qquad L_i = R_{i-1}$$

F-function: $input\ (32\ bits) \rightarrow S_E\ (48\ bits) \oplus subkey\ (48\ bits) \rightarrow S-boxes \rightarrow P \rightarrow output\ (32\ bits)$
Complementary property: if $C = E_K(P)$, then $\bar{C} = E_{\bar{K}}(\bar{P})$.
Attack: Request pairs $C_1 = E_K(P), C_2 = E_K(\bar{P})$, try non-complementary K' values: If $E_{K'}(P) = C_1$, then possibly $K = K'$, and if $E_{K'}(P) = \overline{C_2}$ then possibly $K = \overline{K'}$.

Block Ciphers – Modes of operation

- ECB – Each block is encrypted separately - $C_i = E_K(M_i),\ M_i = D_K(C_i)$
- CBC – Before encryption, each block is XOR'd with the encryption of the previous block -
$$C_i = E_K(M_i \oplus C_{i-1}),\ \ M_i = D_K(C_i) \oplus C_{i-1}$$
- OFB – Compute a pseudo-random string that will be XOR'd to the plaintext -
$$V_i = E_K(v_{i-1}),\ \ C_i = M_i \oplus V_i, \qquad M_i = C_i \oplus V_i$$
- CFB – $C_i = M_i \oplus E_K(C_{i-1}),\ M_i = C_i \oplus E_K(C_{i-1})$

Perfect Cipher

A cipher will be called perfect if every M, C hold $p(M|C) = p(M)$. Equivalent definitions:

$$\forall M, C: p(C) = p(C|M)$$

$$\forall M, C: p(C|M) = \sum_{\left(K \middle| E_K(M) = c\right)} p(K)$$

Therefore, a cipher is perfect iff for all C the above sum is independent of M. A perfect cipher always holds $|K| \geq |M|$.

Unicity distance

$$N = \frac{key\ length\ in\ bits}{D} = \frac{H(K)}{H(C) - H(P)}$$

The unicity distance is the length of M, C in relation to K, that will allow certain identification of the key K given M, C.
H is a measure of mean entropy in a representation of a letter. D is a measure of representation redundancy, and is defined as $D \triangleq H(C) - H(P)$. In English, 1.5 bits are needed for every letter, therefore in ASCII representation for example - $D_{ASCII} = 8 - 1.5$.

Birthday paradox

In order to find collision with probability greater than half, in a function with range of size m, it is enough to draw $1.17\sqrt{m}$ different inputs. (Also works when drawing from 2 different sets)

Groups

A group $\{G,\cdot\}$ holds-

- Closure - $\alpha,\beta \in G \Rightarrow \alpha\cdot\beta \in G$
- Identity element - $e \in G$ such that $\forall\alpha \in G, e\cdot\alpha = \alpha\cdot e = \alpha$
- Inverse element - $\alpha \in G \Rightarrow \alpha^{-1} \in G, \alpha\alpha^{-1} = \alpha^{-1}\alpha = e$
- Associativity– $\alpha,\beta,\gamma \in G \Rightarrow \alpha\cdot(\beta\cdot\gamma) = (\alpha\cdot\beta)\cdot\gamma$

Properties:

$G' \subseteq G$ subgroup iff $G' \neq \emptyset$ (and then $e \in G'$), and the closure property is held on G'. An element's order divides the group's order. If $a^s = e$ then $order(a,G)|s$.

Euler Function

$$\varphi(n) = |\mathbb{Z}_n^*| = |\{i \in \mathbb{Z}_n \mid \gcd(i,n) = 1\}|$$

For $n = \prod_i p_i^{e_i}$:

$$\varphi(n) = \prod_i \left(p_i^{e_i-1}(p_i-1)\right) = n\cdot\prod_i\left(1-\frac{1}{p_i}\right)$$

p, q primes, a, b, n integers. The following holds-

$$\varphi(p) = p-1$$
$$\varphi(p^a) = (p-1)p^{a-1} = p^a - p^{a-1}$$
$$\varphi(pq) = (p-1)(q-1)$$
$$\gcd(a,b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$$
$$\sum_{d|n}\varphi(d) = n$$

$a^p \equiv a\ (mod\ p)$ (Fermat's little theorem)

$$\gcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1\ (mod\ n)$$

Chinese Remainder Theorem

$\mathbb{Z}_{pq}^* \cong \left(\mathbb{Z}_p^* \times \mathbb{Z}_q^*\right)$ and the transition between the groups can be done easily. Alternatively: There exists a homomorphism h: $\mathbb{Z}_{pq}^* \to \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. The homomorphism is defined $h(u) = \left(u(mod\ p), u(mod\ q)\right)$.

Algorithm (for the transition from the right hand side to the left). Calculate a, b such that-

$$a \equiv 1\ (mod\ p) \qquad a \equiv 0\ (mod\ q)$$
$$b \equiv 0\ (mod\ p) \qquad b \equiv 1\ (mod\ q)$$

By $a = q \cdot \left(q^{-1}\ (mod\, p)\right),\ \ b = p \cdot (p^{-1}(mod\ q)$. Then $(s,t) \to a \cdot s + b \cdot t$.

Groups of the form $\mathbb{Z}_n^*$

An element a has an inverse in $\mathbb{Z}_n^*$ iff $\gcd(a,n) = 1$. $order(a, \mathbb{Z}_n^*) | \varphi(n)$, and if n is prime, then $order(a, \mathbb{Z}_n^*) | (n-1)$.
When n is prime and $d|(n-1)$, the number of elements of order d is $\mathbb{Z}_p^*$ is $\varphi(d)$. In particular, the number of generators is $\varphi\big(\varphi(p)\big) = \varphi(p-1)$.
Wilson's Theorem - $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv -1\ (mod\, p)$.

Quadratic residues $(p \neq 2)$

There are $\frac{\varphi(p)}{2} = \frac{p-1}{2}$ quadratic residues in $\mathbb{Z}_p^*$.
Euler's Criterion - $a \in \mathbb{Z}_p^*$ is a quadratic residue iff $a^{\frac{p-1}{2}} \equiv_{(p)} 1$.

For $n = pq$ - if $a \in \mathbb{Z}_n^*$ is a quadratic residue, then it has 4 square roots. Therefore – there are exactly $\frac{\varphi(n)}{4}$ quadratic residues in $\mathbb{Z}_n^*$.

Calculating root modulo p

$p = 4k + 3$ - $\sqrt{a} = a^{\frac{p+1}{4}}$

$p = 4k + 1$ – Probabilistic algorithm –

- Randomly select b which is a quadratic non-residue.
- Initialize $0 \to t,\ \ 2k \to i$
- While i is even
  - $\frac{i}{2} \to i, \frac{t}{2} \to t$
  - If $a^i b^t \equiv -1$ then $t + 2k \to t$
- Return $a^{\frac{i+1}{2}}, b^{\frac{t}{2}}$.

Legendre's symbol

$$\left(\frac{a}{p}\right) \triangleq \begin{cases} +1 & a\ is\ a\ quadratic\ residue\ mod\ p \\ -1 & a\ is\ a\ quadratic\ non\ residue\ mod\ p \end{cases}$$

According to Euler - $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\, p)$
Every c holds $\left(\frac{1}{p}\right) = \left(\frac{c^2}{p}\right) = 1$

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p = 4k+1 \\ -1 & p = 4k+3 \end{cases}$

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

If p, q are odd primes - $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$

Jacoby's symbol

$n = p_1 \cdot p_2 \cdots p_k$ odd. a is coprime to n. Jacoby's symbol is defined as –

$$\left(\frac{a}{n}\right) \triangleq \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

a is a quadratic residue modulo n iff $\left(\frac{a}{p_i}\right) = 1$ for every i. Therefore – if $\left(\frac{a}{n}\right) = -1$ we could know for certain that a is a quadratic non-residue. However $\left(\frac{a}{n}\right) = 1$ does not guarantee that a is a quadratic residue.

1 is a quadratic residue for all n. In particular, $\left(\frac{1}{n}\right) = \left(\frac{c^2}{n}\right) = 1$.

$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

If m, n are coprime and odd - $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{m}{n}\right)$

An efficient search requires $O(\log^2 n)$ modular operations.

Number Theory

a, b coprime $\Leftrightarrow \exists x, y \mid ax + by = 1$
a, b coprime and $a \mid bc \Rightarrow a \mid c$
$m|a, m|b \Rightarrow m|(\alpha a + \beta b) \ \forall \alpha, \beta \in \mathbb{Z}$
$\gcd(a, b) = \min\{ax + by > 0 \mid x, y \in \mathbb{Z}\}$
$lcm(a, b) = \min\{c > 0 |\ a|c, b|c\}$
$m|a, m|b \Rightarrow \ m|\gcd(a, b)$
$\gcd(ma, mb) = |m| \cdot \gcd(a, b)$

Euclidean Algorithm finds gcd, and can be used to find a modular inverse. Complexity $O(\log(n))$.
a has an inverse modulo $n \Leftrightarrow \gcd(a, n) = 1$.

RSA Encryption

p, q large primes, $n = pq$. e coprime to $\varphi(n)$, $d = e^{-1}\big(mod\ \varphi(n)\big)$.
(n, e) public key, d secret.

Encryption $c \leftarrow M^e\ (mod\ n)$. **Decryption** $M \leftarrow C^d (mod\ n)$.
Properties:

Multiplication property - $E(m_1 \cdot m_2) = E(m_1) \cdot E(m_2)$. Encryption preserves Jacoby's symbol $\left(\frac{m}{n}\right) = \left(\frac{m^e}{n}\right)$.
Hardcore bits – lsb, half
Non-trivial element root $(\alpha^2 = 1, \alpha \neq \pm 1)$ allows factorization.
Modular square calculation allows factorization:
if $a^2 = b^2$, then $\gcd(a - b, n)$ and $\frac{n}{\gcd(a-b,n)}$ are the prime factors.

RSA Signatures

- Signing process - $S = D_A(m) = M^{d_A}$
- Verification process - $M =^? E_A(S) = S^{e_A}$

Zero Knowledge Proofs

Perfect – Simulator output with identical distribution to a "real" output.

Computational – The distribution of the simulator output and the distribution of a real prover's output are (computationally) indistinguishable, i.e. there can be a negligible difference between them.

If bit-commitment is used in a ZK protocol, perfect binding must be assured because the prover is computationally unlimited. Therefore the secrecy is computational, and the protocol will be computational ZK rather than perfect.

Zero-knowledge **Computationally**: Graph 3-Colorability.

Differential Cryptanalysis

n-round **Characteristic** is $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)$ such that:

- $\Omega_P - m$ bits, input difference (before encryption)
- $\Omega_T - m$ bits, output difference (after encryption)
- $\Omega_\Lambda = (\Lambda_1, \Lambda_2, \dots \Lambda_n)$ intermediate rounds. Each of them:
  - $\Lambda_i = (\Lambda_I^i, \Lambda_O^i)$ (round input and output, $\frac{m}{2}$ bits each)

And the following are held –

- Λ_I^1 – Right half of Ω_P
- Λ_I^2 - $\Lambda_O^1 \oplus$(Left half of Ω_P)
- Λ_I^n – Right half of Ω_T
- Λ_I^{n-1} - $\Lambda_O^n \oplus$(Left half of Ω_T)
- For every $2 \le i \le n-1, \Lambda_O^i = \lambda_I^{i-1} \oplus \lambda_I^{i+1}$

Correct pair in relation to a characteristic Ω and a key K is a pair of inputs, the difference of which is Ω_P and all the differences in the intermediate rounds match the description in the characteristic.

Probability of a characteristic is the probability that a pair of inputs which matches Ω_P is a correct pair (in relation to all the keys).

Differential is a set of all the characteristics which have identical Ω_P, Ω_T and an equal number of rounds. The probability of a differential is the sum of the characteristics' probabilities.

The iterative characteristic $\Omega_P = (19\ \ 60\ \ 00\ 00_x,\ 00\ \ 00\ \ 00\ \ 00)$, also written as $\Omega_P = (\psi, 0)$. A two-round characteristic, with probability $\frac{1}{234}$. $\Omega_T = (0, \psi)$ so that it can be composed on itself.
Concatenation of the characteristic to 16-17 rounds yields a characteristic with probability of $2^{-62}, 2^{-63}$ respectively.

Note : In order to get the same output of F, two inputs must be different in at least 3 S-boxes.

0R Attack requires $2 \cdot p^{-1}$ pairs of input (p – characteristic probability), from which 2 correct pairs will remain.

Secret Sharing

Secret sharing scheme:

- n parties, each receiving a share.
- A cooperation of pre-defined groups allows to reconstruct the secret.
- Any group that wasn't pre-defined cannot gain any information on the secret.

$(\boldsymbol{k}, \boldsymbol{n})$**-Threshold Scheme** – a group can reconstruct the secret only if its size is at least k.

Hash Function

- Merkle-Damgård padding: Given a message M, M is padded so that its length will be a multiply of the block size. The message length is included in the padding.
- Merkle-Damgård construction: $h_i = H(h_{i-1}, M_i)$, where $h_0 = IV$ and $h(M_1, \dots M_n) = h_n$.

Mutual Commitment

Perfect binding: The committer sends $g^r \ mod \ p$ (r odd/even according to S). The committer cannot cheat (reveal another value), but the receiver can calculate S.

Perfect commitment: sends $g^S h^r \ mod \ p$ (g, h generators of a group of element of order $q|p-1$). The receiver cannot calculate S, but the committer can reveal different S, r values.

Common coin (bit) toss: Each one commits on one bit and sends, afterwards the bits are revealed and the coin will be $b = b_A \oplus b_B$.

OT: B learns a bit with probability $\frac{1}{2}$, A doesn't know whether B has learned the bit.
OT_1^2: B learns one of two secrets of his choice. A doesn't know which secret B has learned.

Implementations: bit commitment, non-interactive zero-knowledge proofs.
